ZyWALL IDP 10

Intrusion Detection Prevention Appliance

Support Notes

Version 1.0

Aug 2004

ZyXEL

Unleash Networking Power

INDEX

Application Notes 4
Deploy IDP 4
Register ZyWALL IDP 10
Firmware Upgrade 16
Signature Update 17
Configure User Defined Policy 18
IDP FAQ 23
What is HIDS? 23
What is NIDS? 23
What is HIPS? 23
What is NIPS (IDP)? 23
What's the difference between false positive and false negative? 23
Is IDP able to investigate VPN traffic? 24
Product FAQ 24
What is ZyWALL IDP10? 24
Why do I need ZyWALL IDP, if I already have ZyWALL 5/35/70? 24
Will I lose network access if my ZyWALL IDP 10 lost power or crash? 24
If I forget IDP's password, how to reset the password to default? 25
How to access IDP through console? 25
How to trouble shoot the false positive and false negative cases? 26
What's the difference between Inline, Monitor and Bypass mode? 26
When should I use VLAN Tag function? 27
How to restart device from WEB GUI, Console? 27
What does "Stealth" mean, why should I need it? 29
I can not remote manage my ZyWALL IDP 10 at home, why? 29
Why should I define Policy Check on WAN/LAN port? 29
What's Pre-defined signature? 30
Why should I need to update signature? 30
Where can I get the description of a policy or advisory? 30
How do I make sure my ZyWALL IDP10 already gets the latest policy? 30
I can't download the latest policy from update server. How can I fix the problem? 31
How many User-defined policies can I have on ZyWALL IDP 10? 32
How many policies does ZyWALL IDP 10 support in total? 32
Does configuration backup include Pre-defined/Updated signatures? 32
What's the default password of ZyWALL IDP10? 32

Why can't I input mail server address by domain name? 32
What's "Drop" and "Block Connection" for Action of User Defined Policy? 33
How to use URL String in Content setup of User-defined policy? 33
What's the definition of "Incoming" and "Outgoing" direction in a policy setup? 33
How to decide which Interface should be applied for policy check? 34
In User-defined policy, what's the meaning of Matching Offset, Matching Depth? 35
How does IDP check multiple contents? 35
What's the priority among Pre-defined policy and User-defined policy? 36
Trouble Shooting 36
Unable to Run Applications 36
CLI Command List 39
System related Command 39
Debug mode CLI Command 42

Application Notes

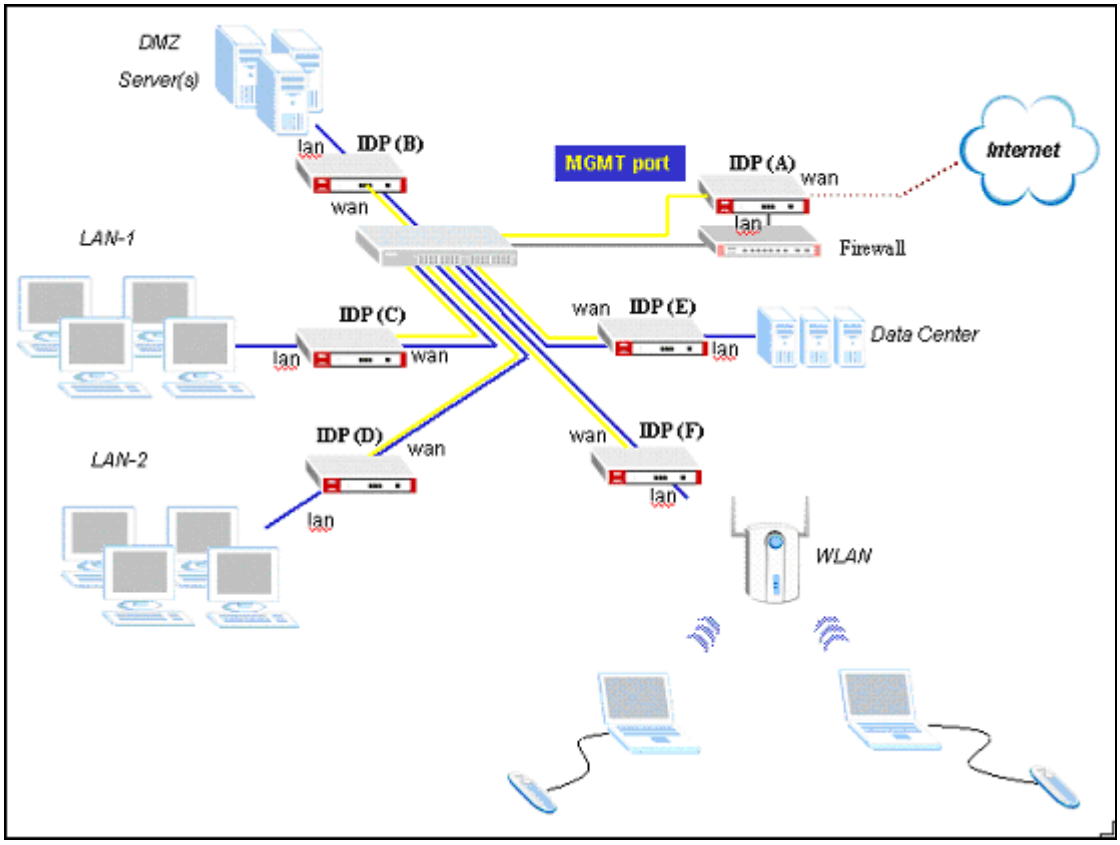
Deploy IDP

IDP functions as a plug and play bridge device filtering malicious traffic from attacking your networks. With continuous signatures update, users can get free from network-based intrusions. In this example, we describe how to deploy and configure ZyWALL IDP10 in a network. Since ZyWALL IDP10 is a bridge device, users don't need to change the existing network topology when they deploy it. Two things matter are

Determine the target network/systems to protect.

Assign an IP address to "Management" port to make management of ZyWALL IDP10 possible in your existing network.

The following diagram and table illustrate the network topology and IP address assignment of the example network.



IP Address assignment:

Network	WAN	DMZ	LAN
Segment	211.1.1.0/28	192.168.2.0/24	192.168.1.0/24

Servers/PC		192.168.2.5-10	LAN1: 192.168.1.5-50 LAN2: 192.168.1.51-100 WLAN: 192.168.1.101-130 Data Center: 192.168.1.131-140
Device	IDP (A)	IDP (B)	IDP (C)
IP Address	192.168.1.141	192.168.1.142	192.168.1.143
Device	IDP (D)	IDP (E)	IDP (F)
IP Address	192.168.1.144	192.168.1.145	192.168.1.146

Purpose:

IDP (A)

Since network devices may also have vulnerabilities, once the firewall device at gateway is compromised, the protected networks are also endangered. The IDP device outside firewall can block attacks to firewall/VPN gateways from Internet. So we apply policy protection on WAN port of IDP (A).

IDP (B)

Servers in DMZ zone are the most critical point in your network. Since malicious attacks may flow into DMZ along with legitimate traffic. The attacks may come from Internet and to prevent the infected server from attacking internal networks, so we apply policy protection on both WAN and LAN port of IDP (B).

IDP (C), IDP (D)

The purpose of IDP (C) and IDP (D) is to separate internal network into blocks, and thus once a PC gets infected by some worms/virus, the infection won't spread into the whole network. Therefore we apply policy protection on both WAN and LAN port of IDP (C) and IDP (D).

IDP (E)

Since IDP (E) protects the data center of the network, and we assume data center is always waiting for internal users to access, there are no connections initiated from the data center area. We apply policy protection on WAN port of IDP (E).

IDP (F)

Wireless LAN is a popular application nowadays due to its mobility. However, WLAN does raise some security concerns into network applications also because of its mobility. Administrators can't predict when a mobile notebook will be cracked, and trying to spread worms/virus through WLAN. So we suggest users to place an IDP device before WLAN connects to internal network. The policy protection applies on LAN port of IDP (F).

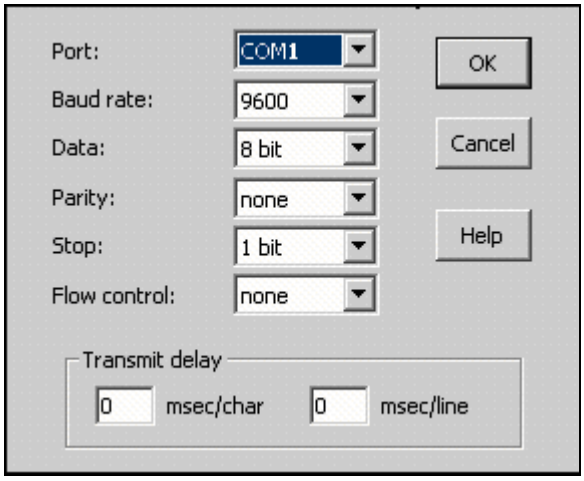
Setup IP address of IDP (A, B, C, D, E, F)

1. Configure each IDP device's IP address.

Since IDP is a bridge device, it only has one IP address for management purpose, IDP also uses this IP address to update signatures and the send system logs through syslog/E-mail/FTP. To configure the system IP address of IDP device, users can choose two methods,

- Through Console

1. Make sure the baud rate/data/parity/stop/flow control settings are as below.



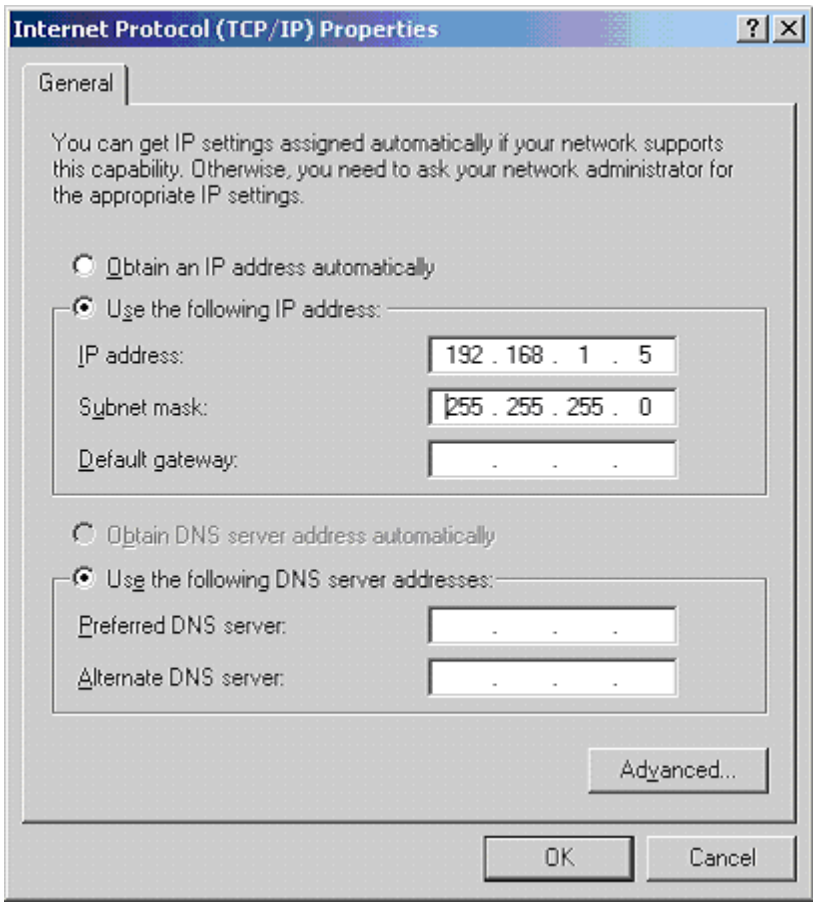
2. Default Login/password is "admin/1234"
3. Issue the following commands on IDP (A)

```
$>set system ip 192.168.1.141

Change ZyWALL IDP 10 IP address OK.
$>set system mask 255.255.255.0

Change ZyWALL IDP 10 netmask OK.
$>set system gateway 192.168.1.254

Change ZyWALL IDP 10 default gateway OK.
$>set system dns 168.95.1.1

Change ZyWALL IDP 10 default DNS server OK.
```

4. Repeat the step 3 to configure IDP (B, C, D, E, F) according to IP address assignment table.

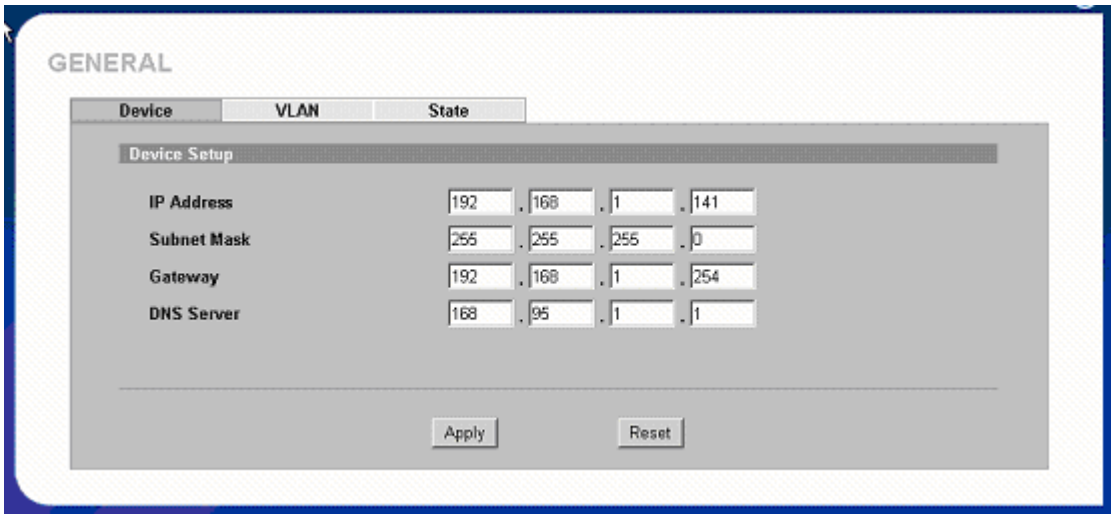
- Through WEB GUI or Telnet

1. Connect one PC to IDP's management port by crossed Ethernet cable. Make sure MGMT port light is on.
2. Go to Start->Settings->Network and Dial-up Connections, and select the Ethernet connection you are connecting to IDP device.
3. Change PC's IP address to 192.168.1.5, subnet mask= 255.255.255.0 from properties.



4. Log into IDP's WEB GUI via browser.

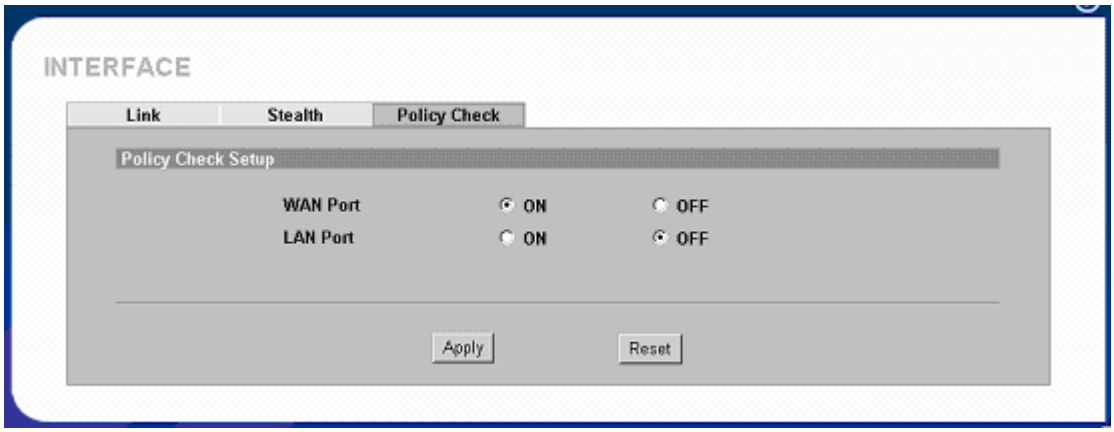
5. Go to SYSTEM->General->Device, input IDP (A,)'s IP address, subnet mask, default gateway, DNS server's IP address.



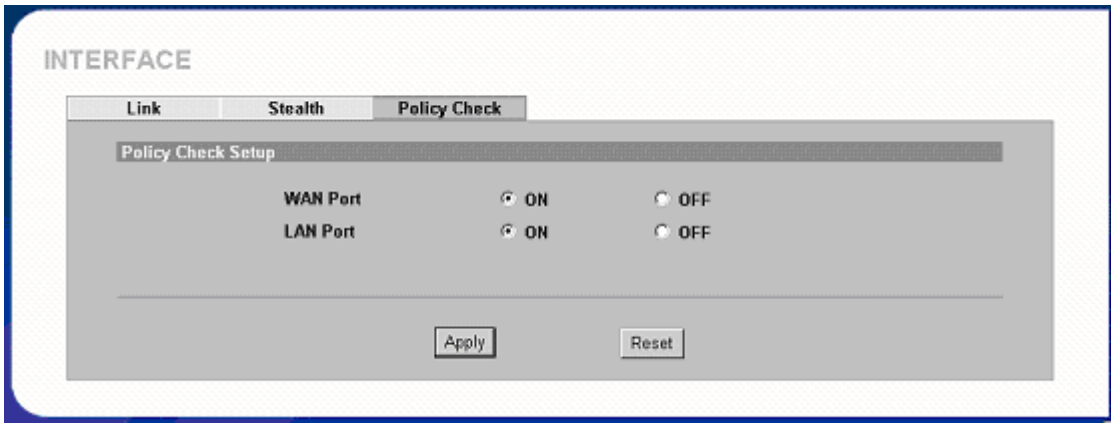
6. Repeat step 1-5 to configure IDP (B, C, D, E, F) according to IP address assignment table.

Connect the MGMT/LAN/WAN ports of all IDP devices to the network according to the deployment topology (192.168.1.0/24).

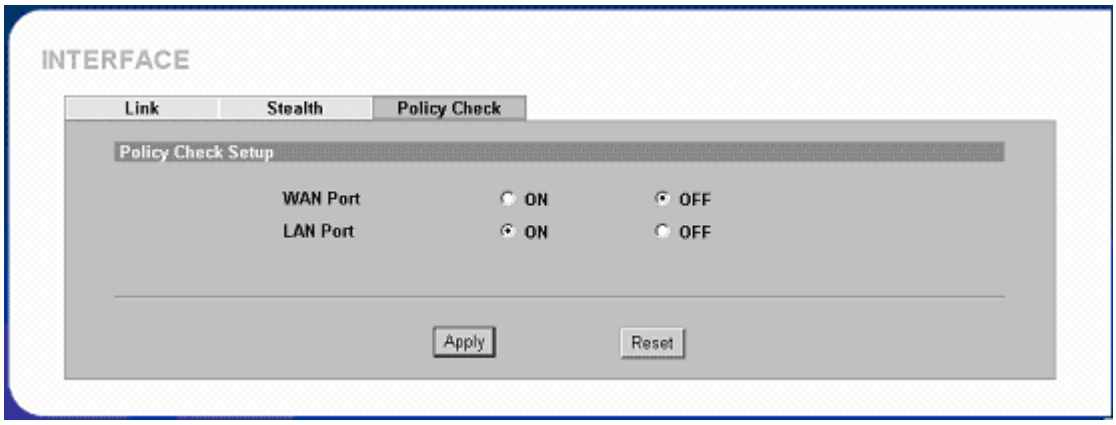
Login IDP (A, E)'s WEB GUI; go to SYSTEM->INTERFACE->Policy Check. Then enable policy checking on WAN port of IDP (A, E).



Login IDP (B, C, D)'s WEB GUI, go to SYSTEM->INTERFACE->Policy Check. Then enable policy checking on WAN and LAN port of IDP (A).



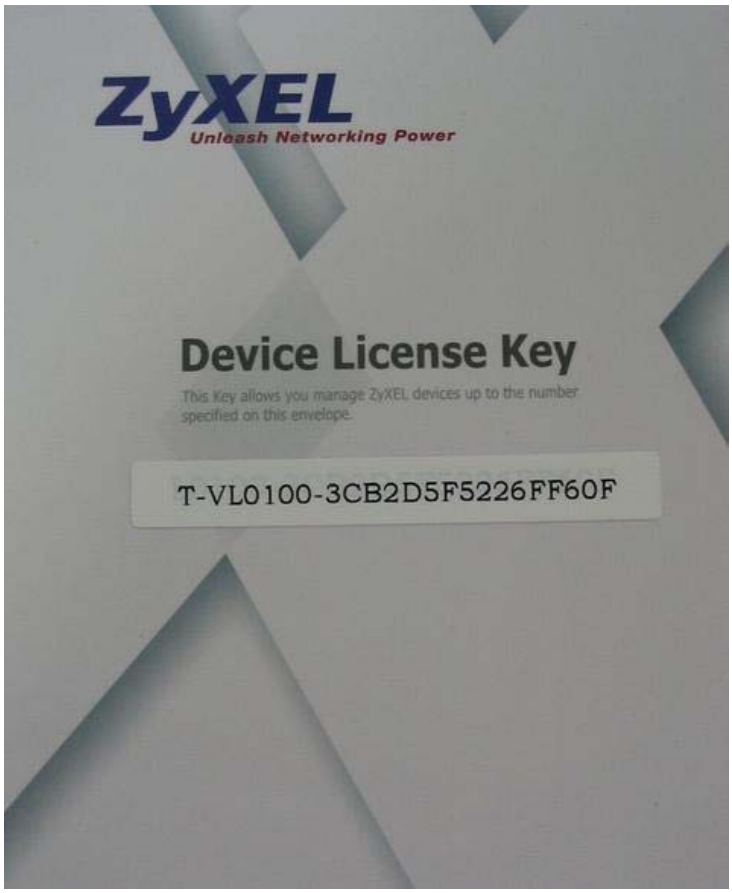
Login IDP (F)'s WEB GUI; go to SYSTEM->INTERFACE->Policy Check. Then enable policy checking on LAN port of IDP (F).



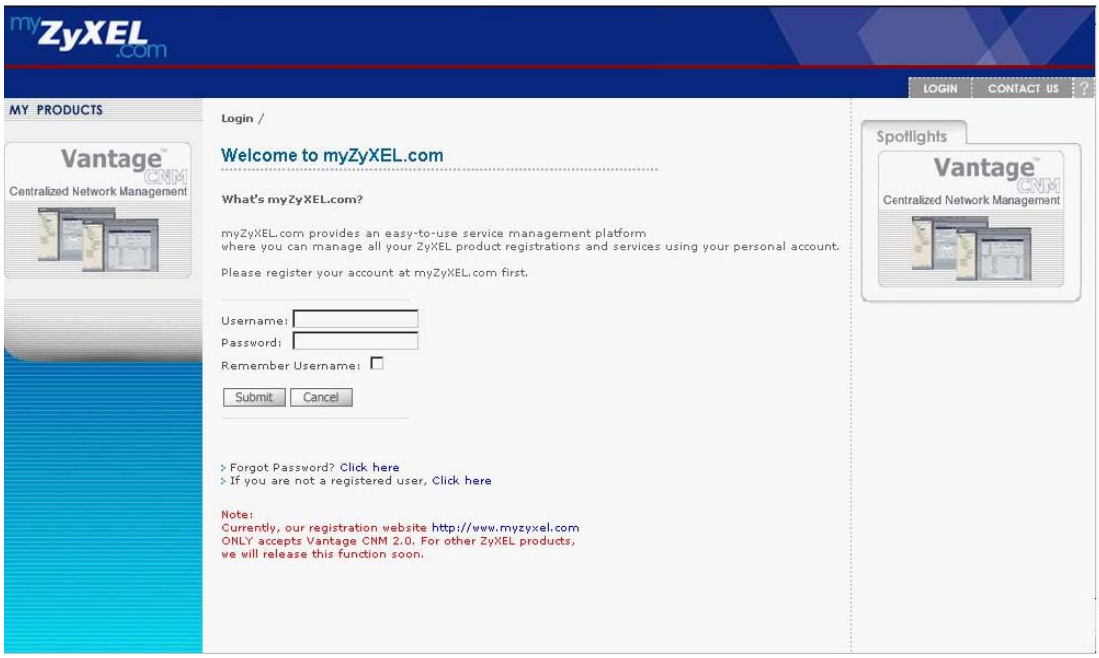
Register ZyWALL IDP

ZyWALL IDP comes with a “pre-defined” policy set which requires subscription and can be update at regular bases. Having an up-to-date policy set is essential as new attack types evolve.

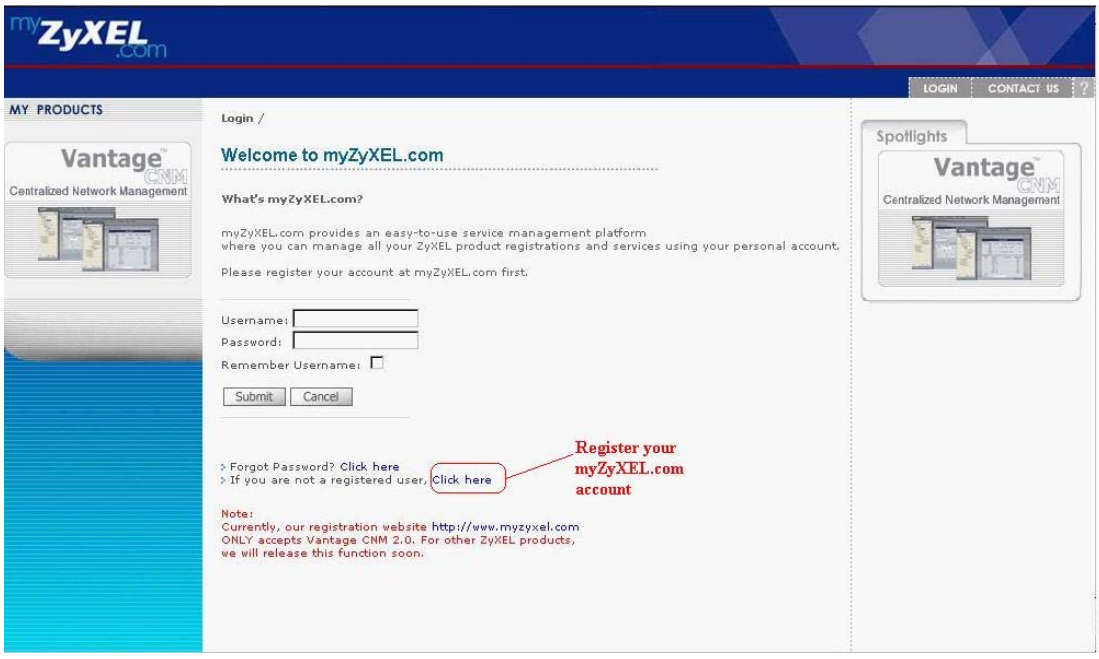
1. A “Device License Key” card is included in ZyWALL IDP package for one year free subscription.



2. Go to ZyXEL Communications online services center. http://www.myZyXEL.com.

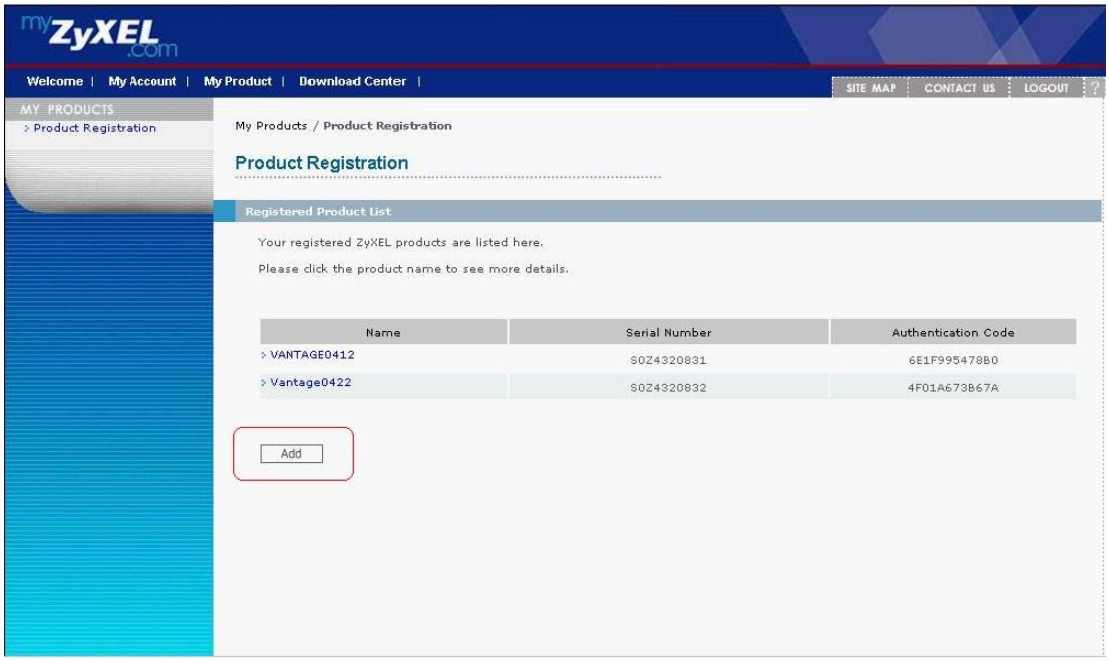


3. In case you haven't got an account on myZyXEL.com, you need to get a new account. Please follow the instruction on myZyXEL.com; we skip the description of detailed procedure in this article. If you get into trouble in this step, please contact ZyXEL support.

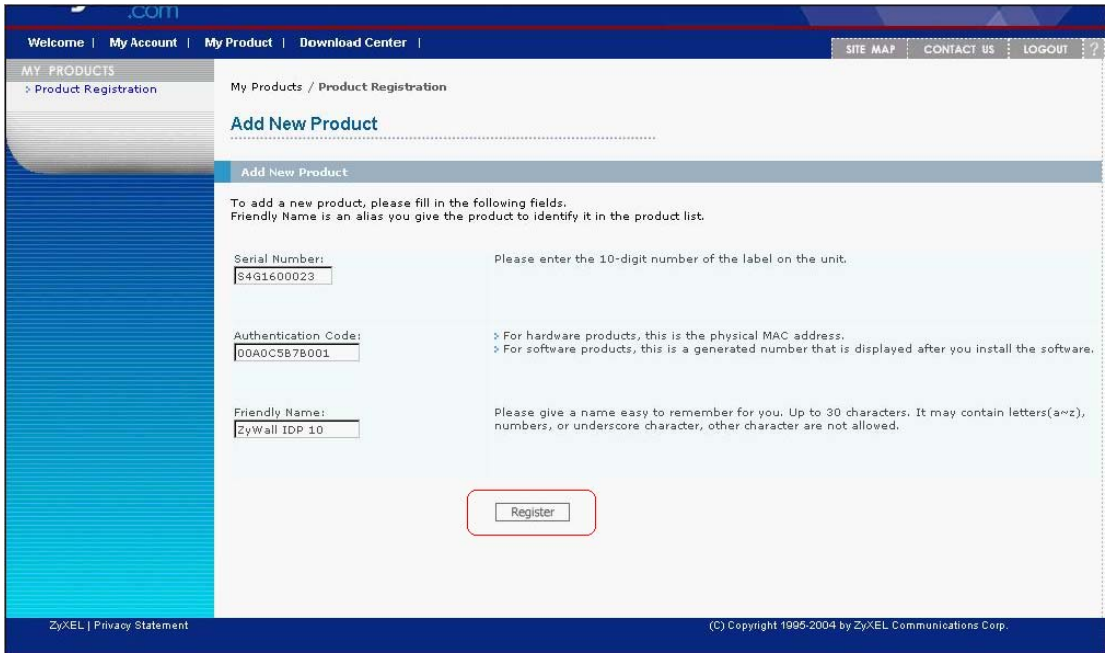


4. Login into myZyXEL.com using your account. “Click here” to register **ZyWALL IDP**.

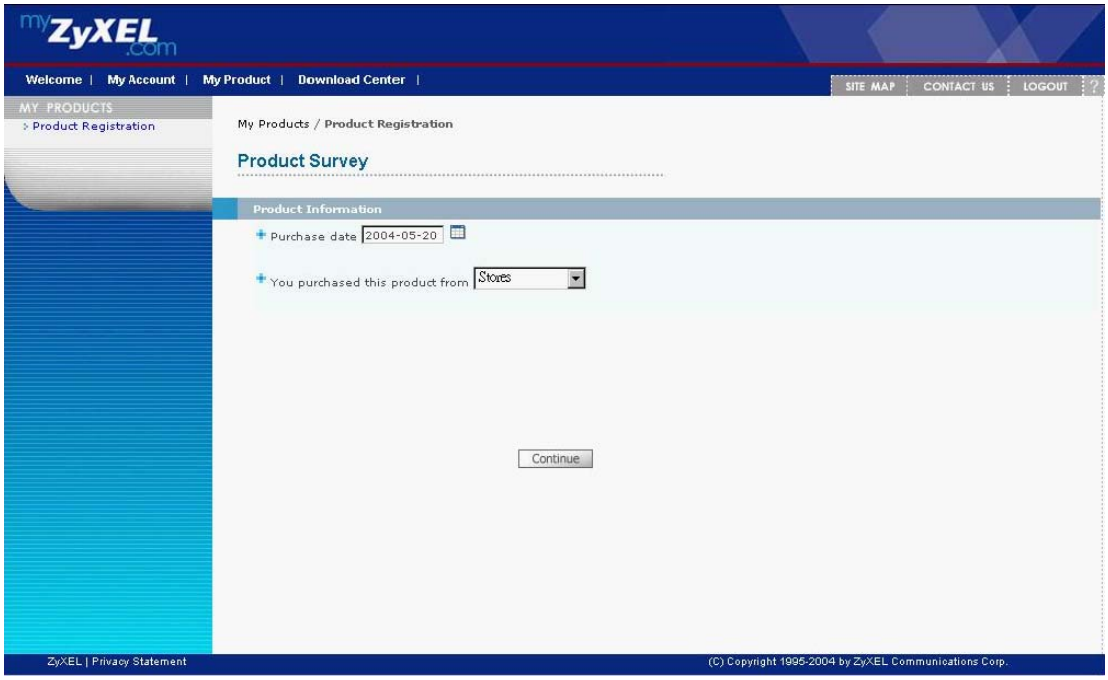
5. Press **add** button to add the **ZyWALL IDP** you have.



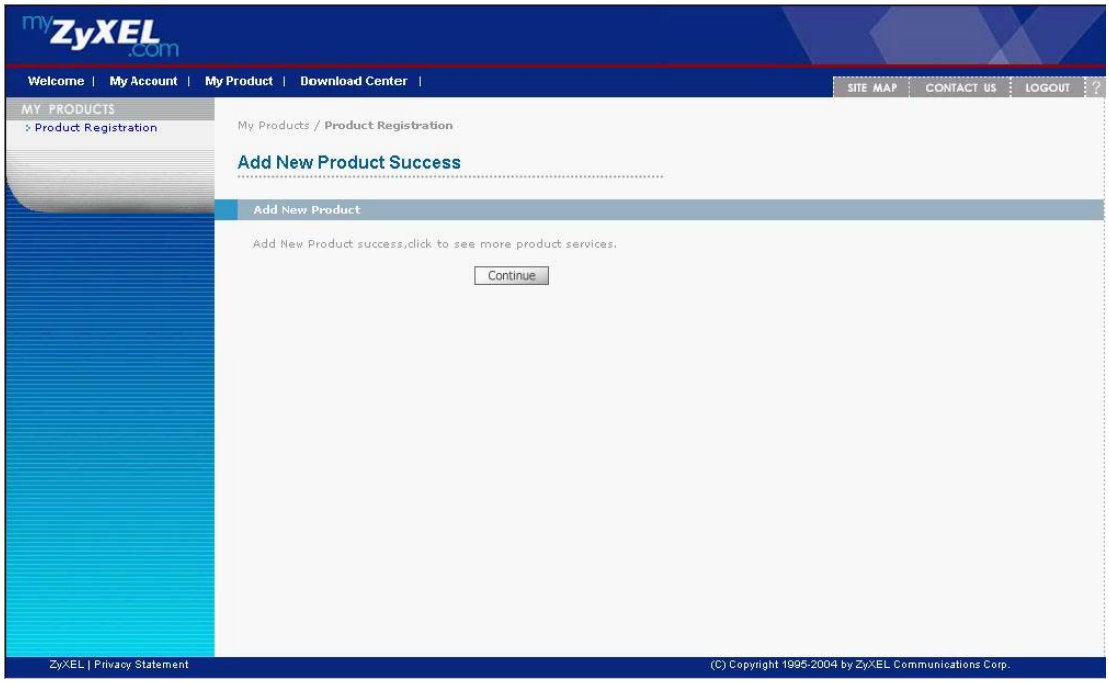
6. In this step you need to enter **Serial Number**, **Authentication Code** (MAC address), and a Friendly Name for your product. You can find **serial number** and **MAC address** at the bottom of your device.



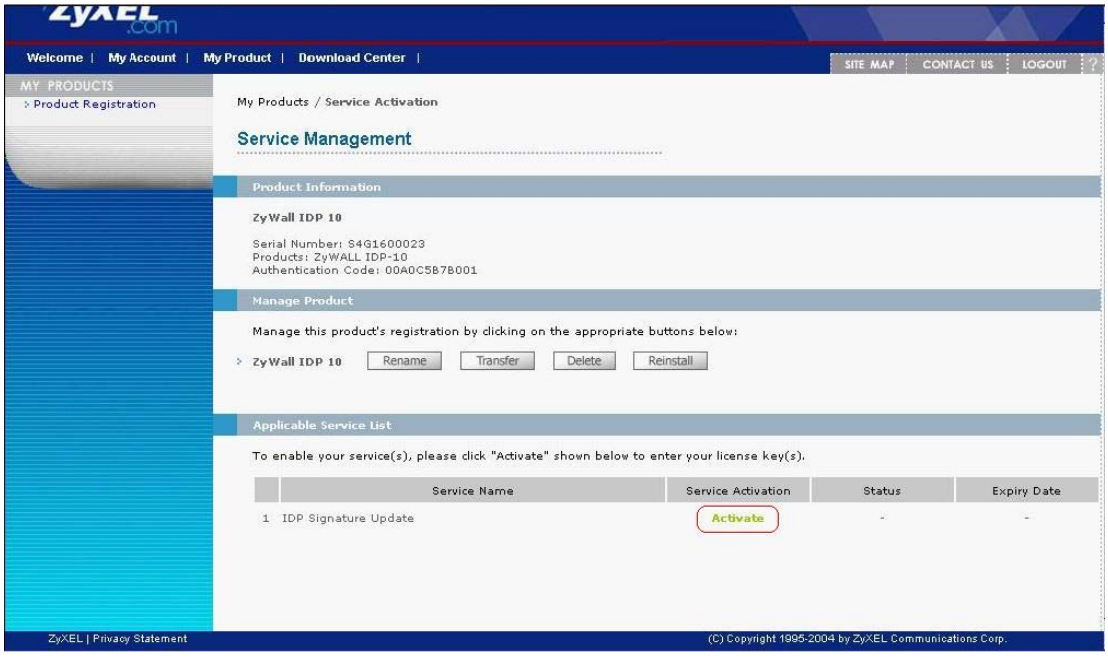
7. Input the date you purchase the product, and the purpose of the buying.



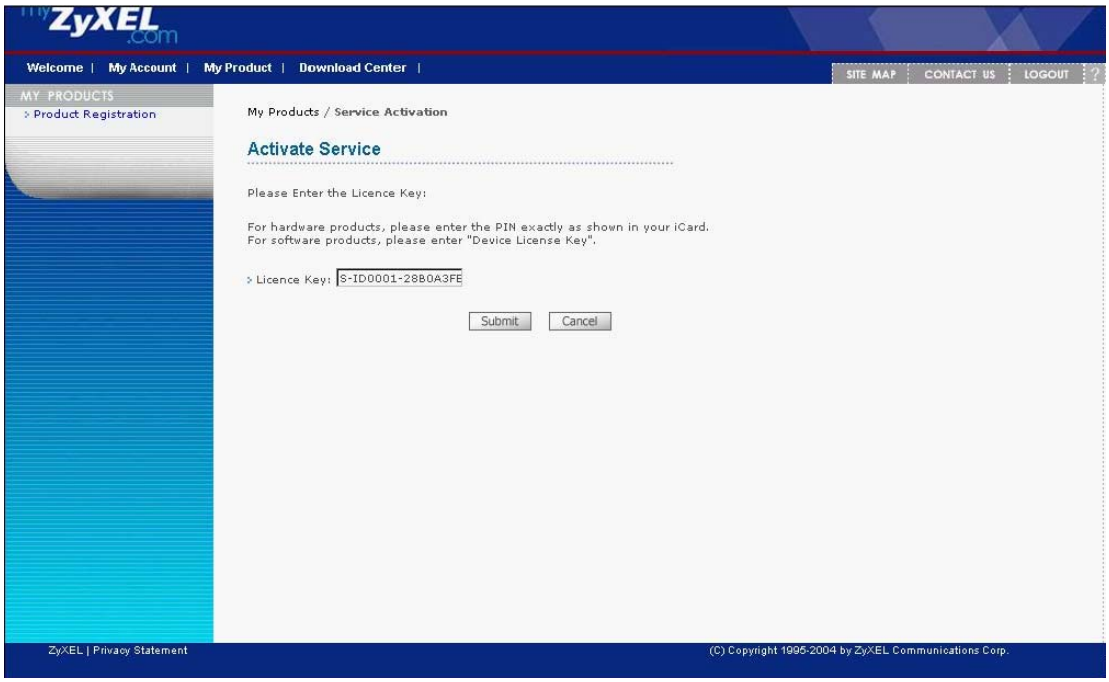
8. You would get a successful message. Then press Continue button.



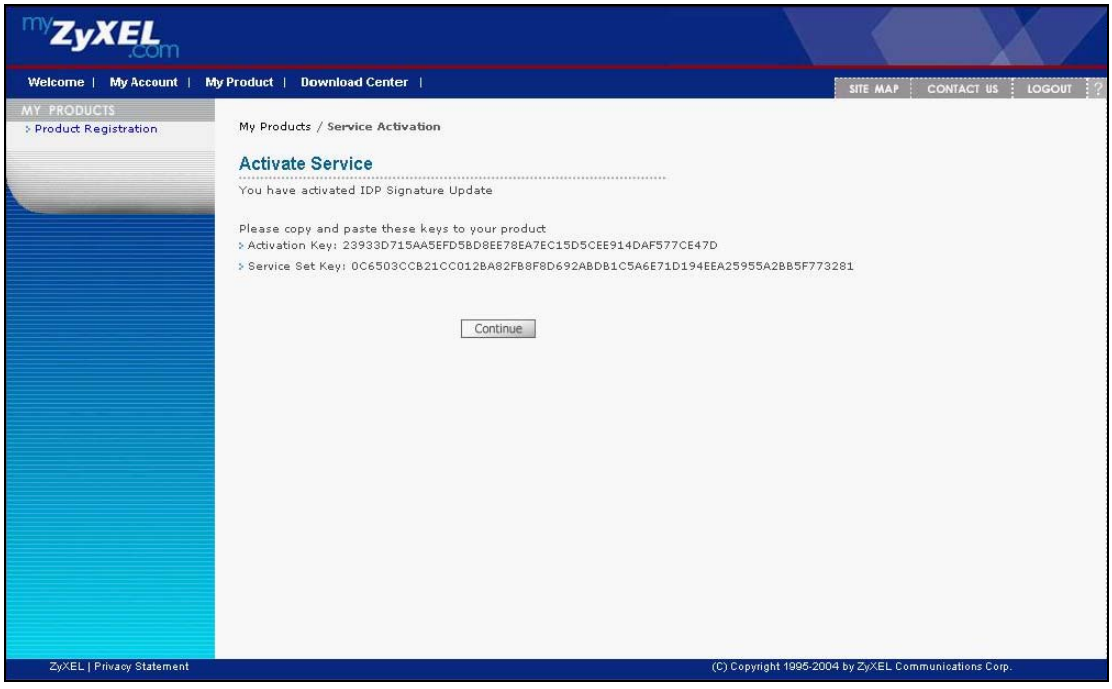
9. From ZyWALL IDP's Applicable Service List, you will have a service "IDP Signature Update" available. Click **Activate.**



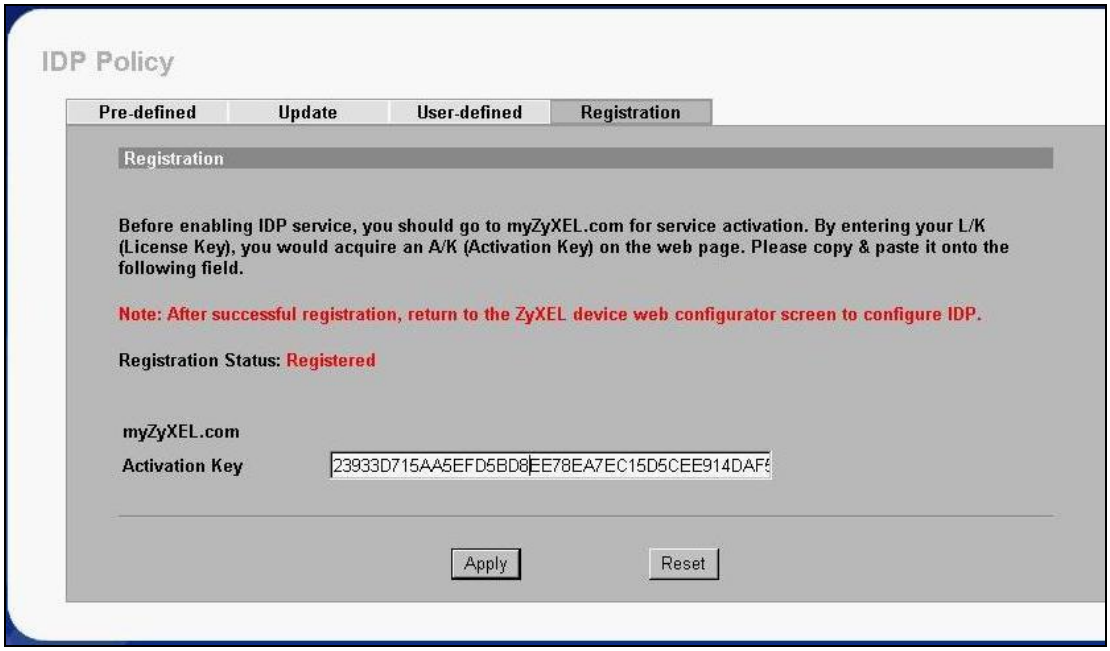
10. Enter the license key you get from "**Device License Key**" card. Then press **Submit** button.



11. After clicking **Submit** button, you will get an "**Activation Key**" and "**Service Set Key**". An email with these keys will be send to your email address as well.

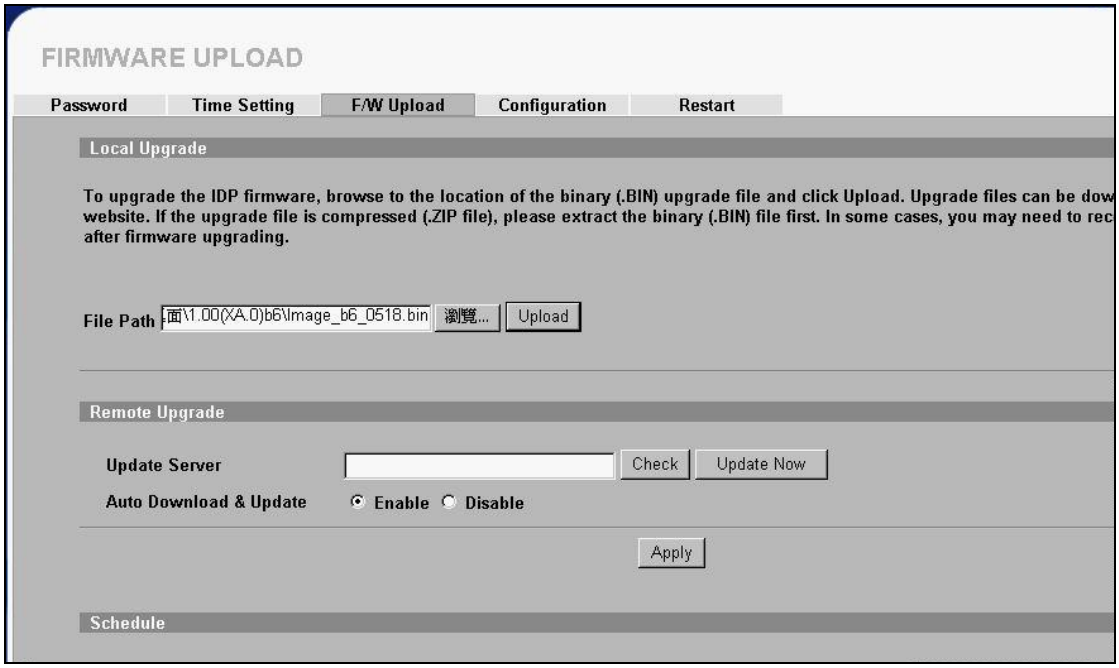


12. You can copy & paste "**Activation Key**" to ZyWALL IDP's Registration page.

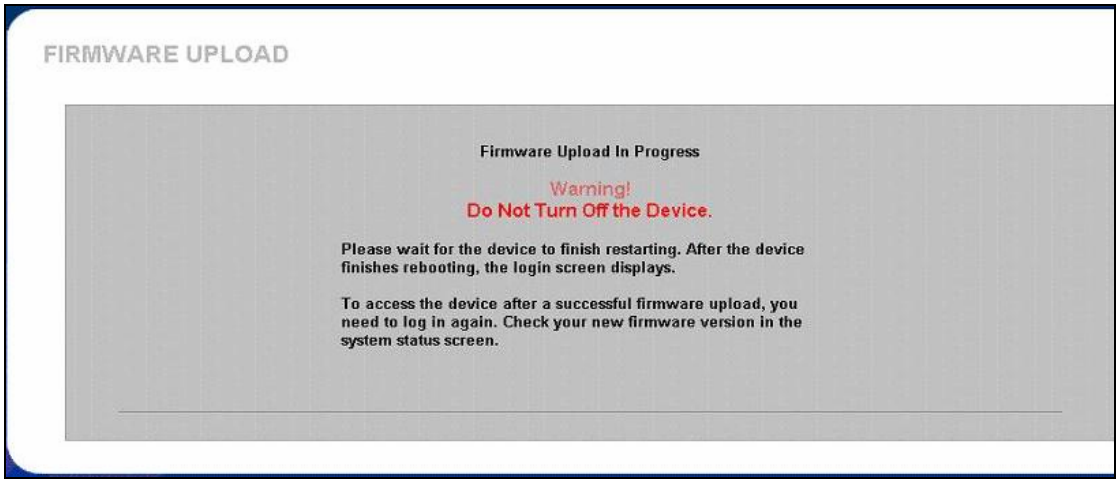


Firmware Upgrade

1. Under Maintenance you can find F/W Upload tab.
   Click browse to select firmware file (.bin) and click Upload button to start firmware upload.

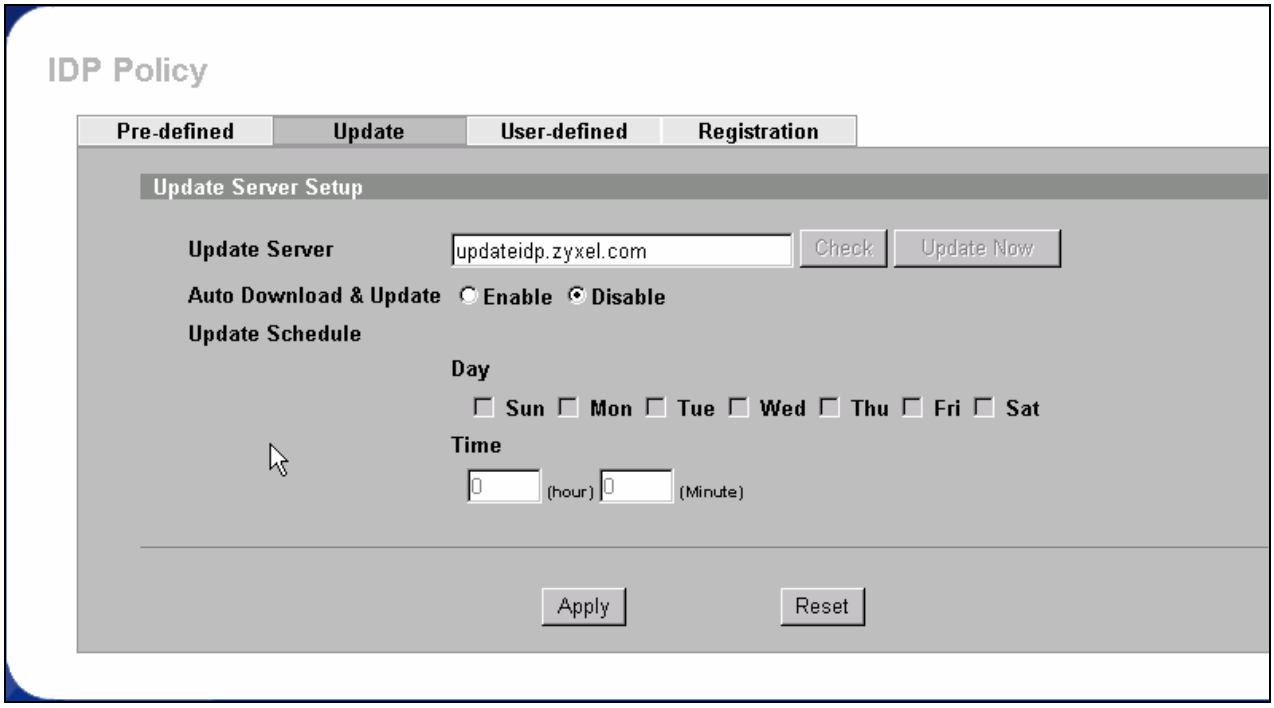


2. It may take few minutes for firmware upload process to finish.
   ZyWALL IDP will reboot when firmware upload completed.

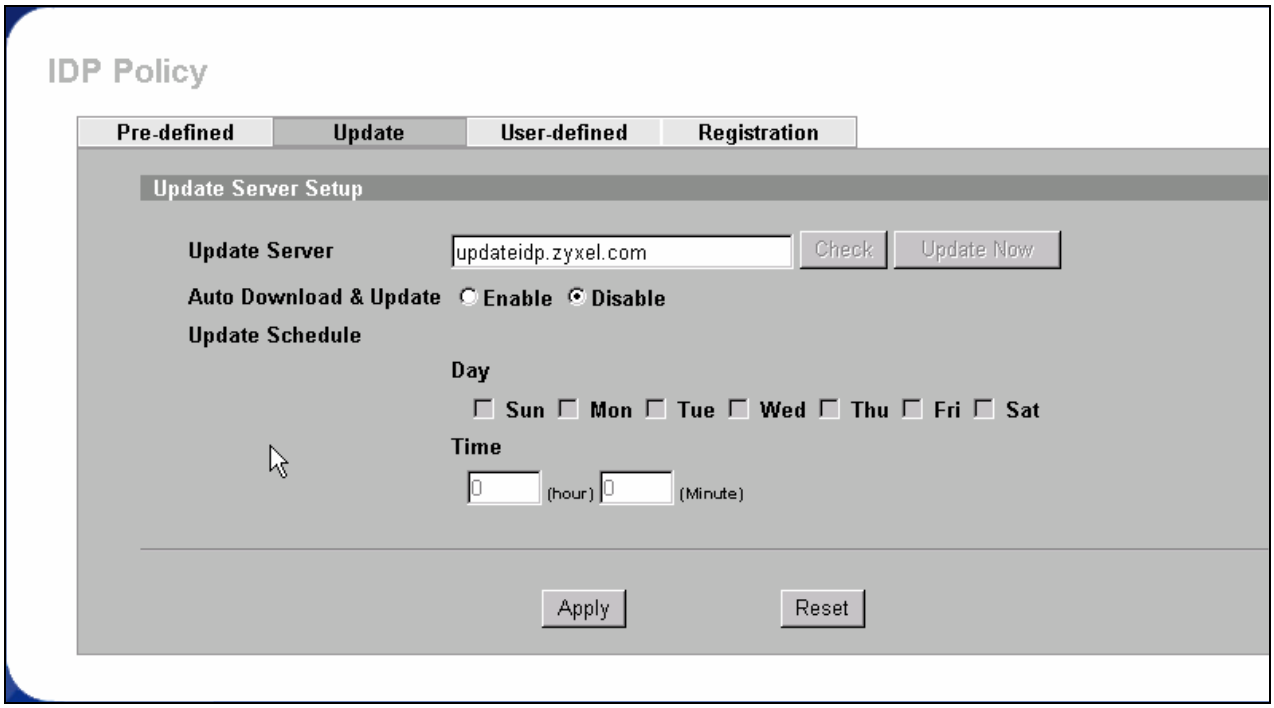


Signature Update

*Make sure you have registered your ZyWALL IDP before you do the signature update.
To update pre-defined policy for your ZyWALL IDP, login into ZyWALL IDP via HTTP, go to IDP > Update and enter Update Server's domain name (updateidp.zyxel.com)
1. You could click Update Now to force ZyWALL IDP to perform signature update immediately.



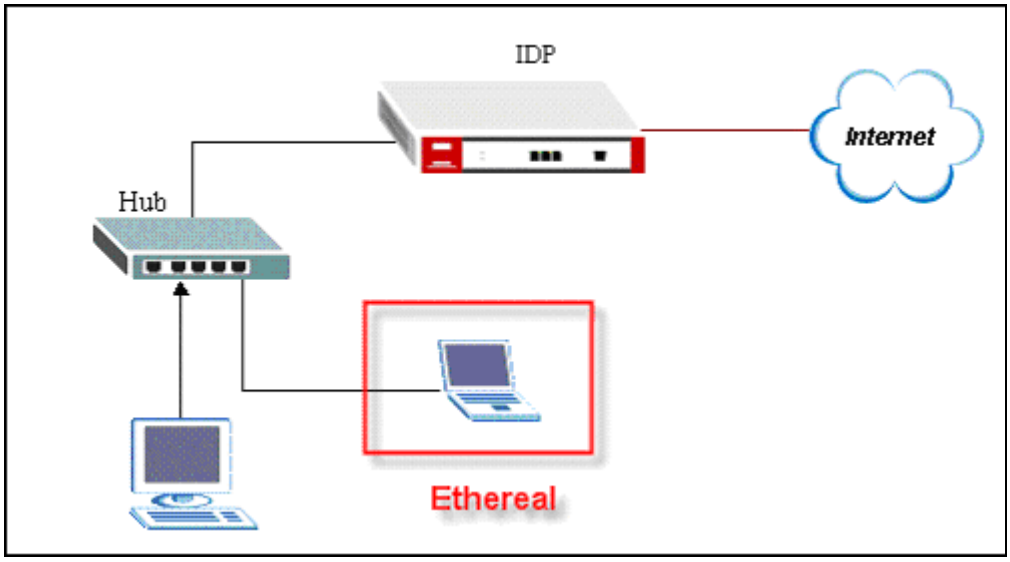
2. Enable "Auto Download & Update" if you want to perform update during non-peak hour.



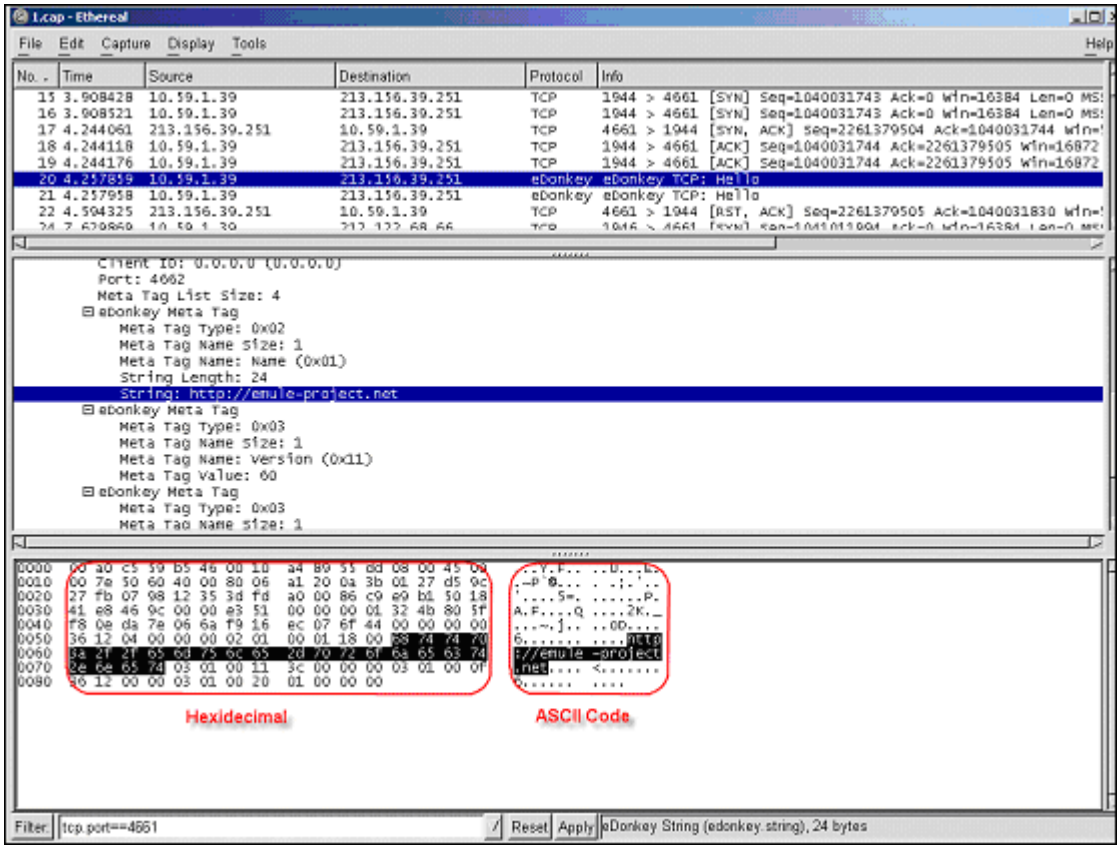
Configure User Defined Policy

In this example, we describe the procedure of using user defined policy. We take eMule application as an example. eMule is a P2P file sharing application. In the following description we break down the procedure of how to get and analysis eMule traffic pattern, and how to setup user defined policy in IDP.

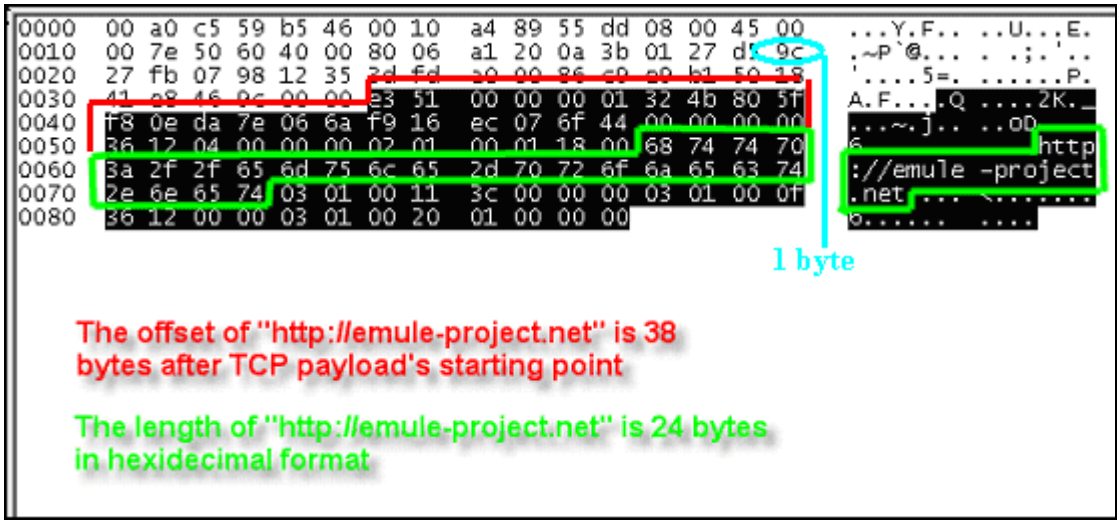
1. Get Ethereal installed on a PC. Ethereal is a freeware packet capturing tool, you can get a freed download from http://www.ethereal.com.
2. Insert a hub where the ethereal traffic flows.
3. Attach the PC with Ethereal installed on the hub as below.



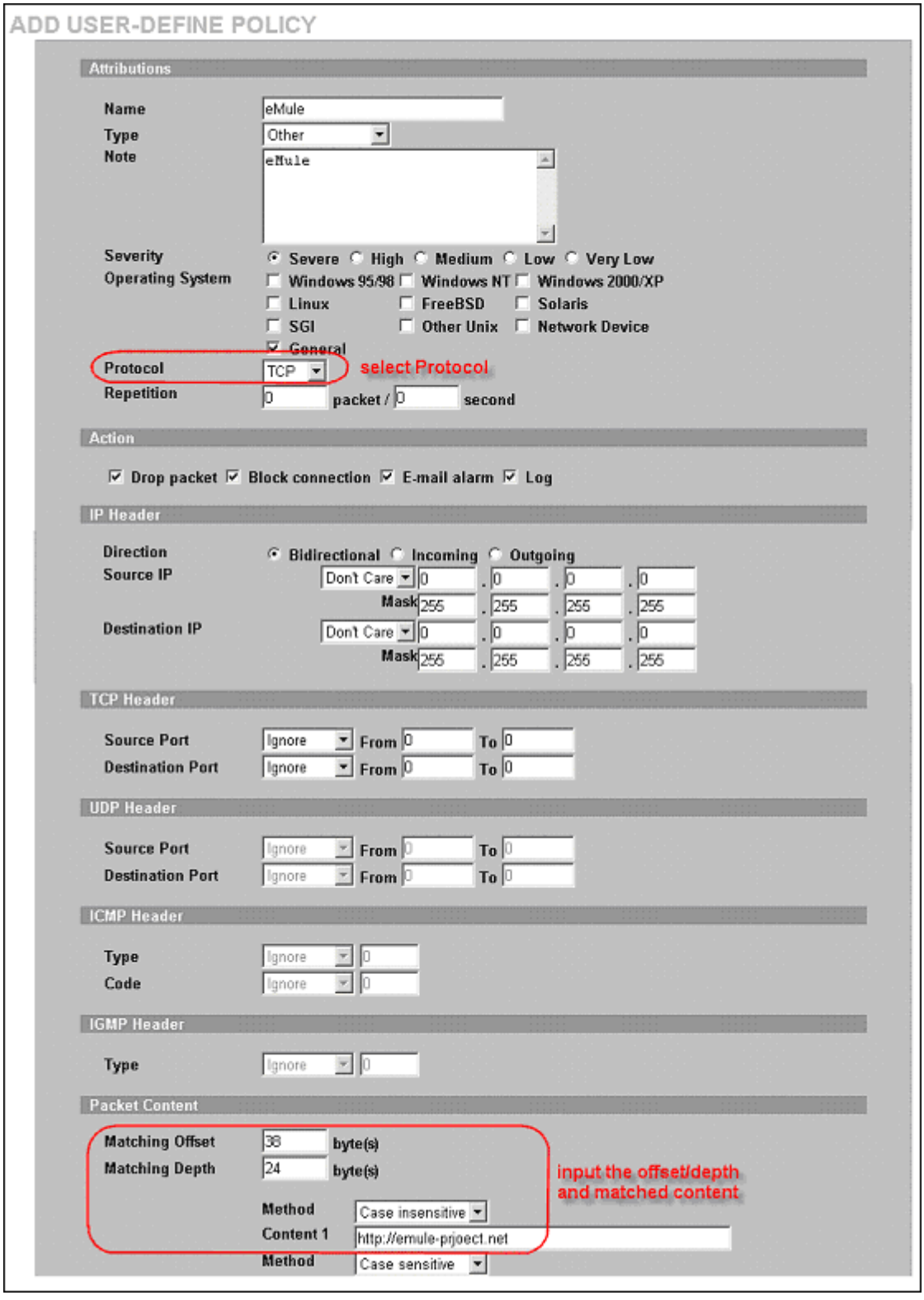
4. Start ethereal packet capturing.
5. Initiate eMule connection from the internal PC, be sure to reduce unnecessary traffic if possible.
6. Stop packet capturing.
7. Analyze the packet. In ethereal, you will get 3 sub-windows. The first window displays summary of each packet in time sequence. In the second window, you can check the parsed details of the selected packet. In the third window, the selected packet is displayed in Hexadecimal and ASCII format respectively. The basic level to analyze a connection's pattern is to trace the ASCII format of the packet. After observing, we can see eMule client sends "eDonkey TCP: Hello" after TCP three way handshaking. And each time, you can see the key word of "http://emule-project.net" appears in TCP payload.



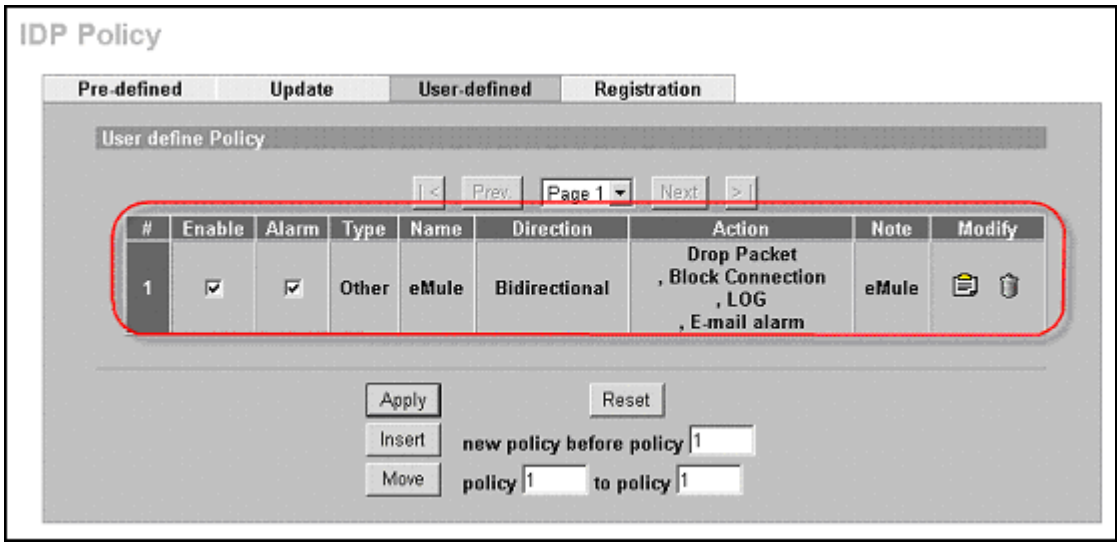
8. Count the TCP offset and the length of “http://emule-prjoect.net”



9. Create User-defined policy in IDP. Login to IDP’s WEB GUI; go to IDP->User-defined. We’ll create a user-defined policy for TCP protocol, with offset=38 bytes, matching depth=24 bytes. Please note that the starting point of offset depends on which protocol you select. For TCP (UDP/ICMP) protocol, the offset starts from the starting points of TCP (UDP/ICMP) payload. IP and TCP (UDP/ICMP) headers are not included. For IP protocol, the starting point of the offset is at the end of the IP header (IP header is not included). Press **Apply** button to save the policy.



After click **Apply** button, we get the summary of the user defined policy.



IDP FAQ

What is HIDS?

Host intrusion detection systems are intrusion detection systems that are installed locally on host machines. This makes HIDS a very versatile system compared to NIDS. HIDS can be installed on many different types (roles) of machines namely servers, workstations and notebook computers. This methodology gives an organization the edge where as an NIDS will fail if it has to reach a segment beyond NDIS capability.

What is NIDS?

Monitors all network traffic passing on the LAN segment where NIDS is installed; reacting to any anomaly or signature based suspicious activity. Think of it as a packet sniffer that analyzes every packet for attack signatures.

What is HIPS?

A Host Intrusion Prevention System resides on the network host protecting it from attack. These used to be known as personal firewalls but as their capabilities increased the HIPS term took hold.

What is NIPS (IDP)?

Intrusion means someone intentionally break into your computer/network, either to steal your confidential data or do something to your computer/network that is against your will. Unlike traditional IDS (Intrusion detection system) only detects suspicious packets; IDP takes it to the next level, it can blocks/drops the malicious packets.

What's the difference between false positive and false negative?

A false positive is when a IDS/IDP system incorrectly reports that it has found attacks, and falsely drops a legitimate packet. But if an attack can through IDS/IDP system without being awared, then we call it's a false negative.

Is IDP able to investigate VPN traffic?

No, VPN traffics are encrypted, IDP is not able to decrypted VPN traffics, and thus it could not investigate VPN packets.

Product FAQ

What is ZyWALL IDP10?

ZyWALL IDP10 functions as a plug and play bridge device filtering malicious traffic from attacking your networks. With continuous signatures update, users can get free from network-based intrusions.

Why do I need ZyWALL IDP, if I already have ZyWALL 5/35/70?

ZyWALL 5/35/70 work as layer 3/4 firewalls, which can block traffic based on source/destination IP addresses, protocol number, and source/destination ports. With stateful packet inspection, the response traffic can be successfully forwarded while traffic initiated from outside can be blocked. And ZyWALL 5/35/70 can protect your network from network based DoS attacks, such as TCP synch flood, ping of death, IP spoofing…etc.
A common misunderstanding is that firewall recognizes all kinds of attacks and can block them. However, attacks nowadays may flow into trusted network through legitimate ports forwarded on firewall devices.
Located at the boundary to your network, firewall can be a gate-keeper from your network to Internet; however, it's not enough to protect your network from being hacked inside the network.
Some reasons for adding IDS to your firewall are:

- Double-checks mis-configured firewalls.
- Catches attacks that firewalls legitimate allow through (such as attacks against web servers).
- Catches attempts that fail.
- Catches insider hacking.

Will I lose network access if my ZyWALL IDP 10 lost power or

crash?

ZyWall IDP 10 does not support hardware bypass, so if your ZyWALL IDP 10 lost power or crashed, you will need to either replace it or take it off the network immediately.

If I forget IDP's password, how to reset the password to default?

The default IDP user name/password is "admin/1234". Customers can modify the default user name/password for security reason. But sometimes users may forget their user name/password, when this happens, please follow these steps to reset configuration on the device.
Connect IDP device through console.
Go to debug mode, issue reset command to reset all settings (not including default policies and user defined policies).
Reboot the device by reboot command.

```
ZyXEL system kernel loader v1.0.0.0 2004/04/02 (ZyXEL)
Press ENTER to enter Debug Mode

Enter DEBUG Mode                    Press Enter
.....
Loading Kernel Image <DBGBOOT>
.....
Checksum is valid.
Starting address is at 0x100000
Kernel image load completed.
Starting kernel...

ZyXEL -- DebugKernel Version 1.0.2 (2004/04/29)

$>resetAll

Are you sure to reset all settings to manufacturing defaults? (y/n)y
Reset to defaults OK. Please reboot to apply new change.
$>reboot
```

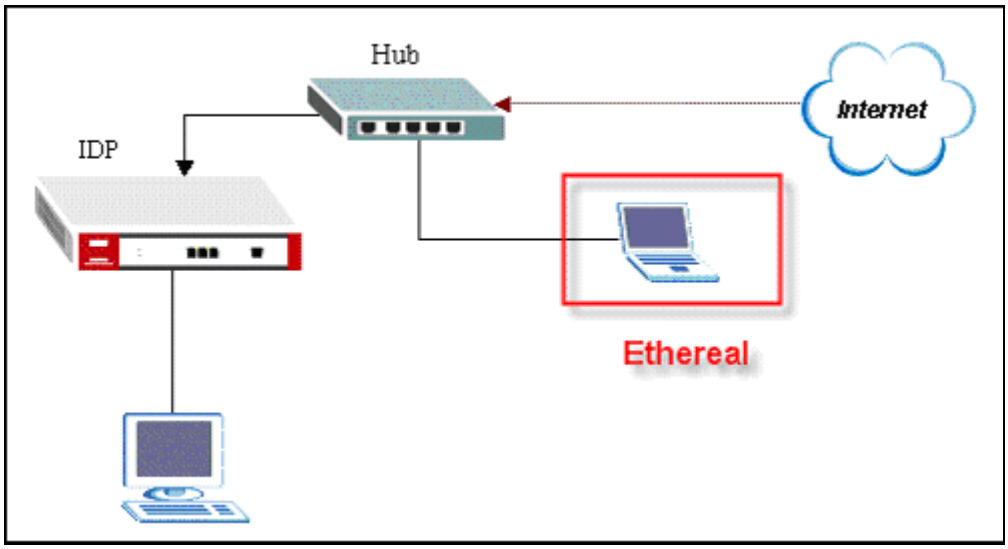
How to access IDP through console?

To access the IDP via console port, a computer equipped with communication software such as HyperTerminal must be configured with the following parameters.
VT100 terminal emulation

9600bps baud rate
N81 data format (No Parity, 8 data bits, 1 stop bit)
The baud rate of IDP10 is unchangeable.

How to trouble shoot the false positive and false negative cases?

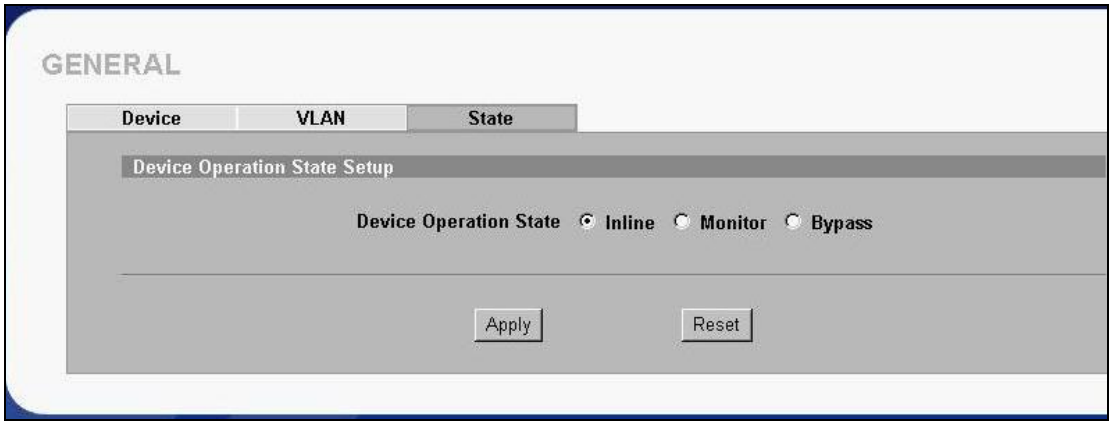
Please capture the problematic packets through the following steps and send the packet trace back to ZyXEL support. The capturing can be done as follows:
Prepare a PC with a packet capturing software. (Go to http://www.ethereal.com for free download.)
Calibrate time on PC and IDP.
Put the PC on IDP-10's interface where the problematic packets arrive.



Observe the log on IDP where the false positive/negative logs occur and save the packets captured by the Ethereal at that timestamp.

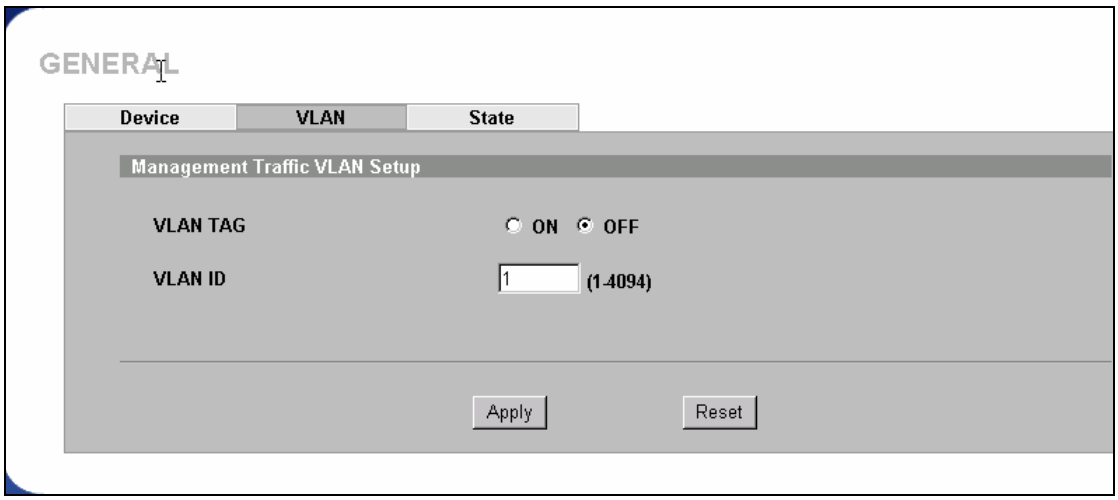
What's the difference between Inline, Monitor and Bypass mode?

Inline: Put ZyWALL IDP in action! It detects any suspicious or malicious packets running through it, and depends on the action policy, it would log, drop, or blocks the packets.
Monitor: ZyWALL IDP monitors all the traffics going through it, but does not block any packets. Think of it as a surveillance camera. It's recommended to have your ZyWALL IDP in **monitor** mode when you fist install it to your network. You could then identify and correct any "false positive: or "false negative" detections
Bypass: ZyWALL IDP will not detect nor block any traffic at all.



When should I use VLAN Tag function?

Virtual LAN, a groups of network devices (PC, router, etc…) that behave as if they are connected to the same wire even though they may actually be physically located on different segments of a LAN.
If the computer you use to manage ZyWALL IDP is in LAN with VLAN ID3, you must configure your ZyWALL IDP with VLAN ID3.



How to restart device from WEB GUI, Console?

WEB GUI

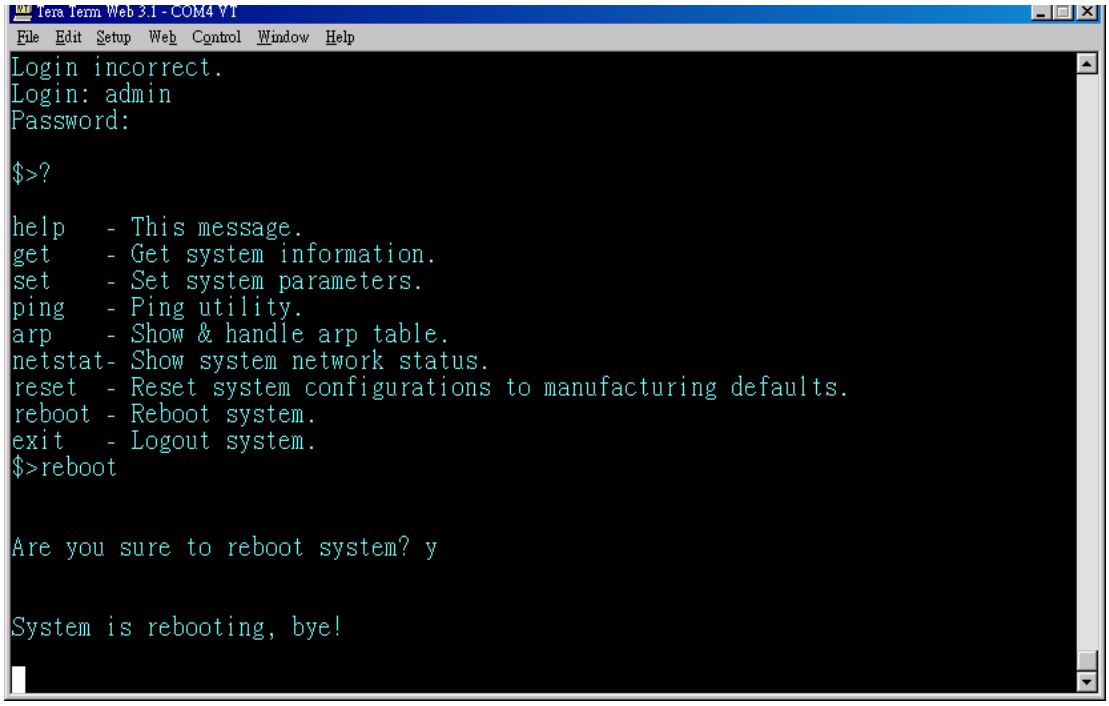
Login to your ZyWALL IDP using an internet browser

Select Maintenance from the menu, and click Restart Tab

Click Restart button to restart your ZyWALL IDP. It may take few minutes before you can access the device again.

Console

Login using admin/1234, and type the command “reboot” to restart your device.



What does "Stealth" mean, why should I need it?

When you enable **Stealth** mode on an interface (WAN/LAN/MGMT), it will not respond to any type of traffic intended for it; it will not respond to traffic like ICMP echo request.
Before hacker/cracker could infiltrate your network, hacker/cracker would need to take down your ZyWALL IDP before attacking your internal network. Configure your ZyWALL IDP's interfaces in **Stealth** mode, so hacker/cracker would not be able to attack it.

I can not remote manage my ZyWALL IDP 10 at home, why?

By default, ZyWALL IDP 10's WAN port is in Stealth mode to prevent hacker from entering ZyWALL IDP 10. It's recommended always use MGMT port to configure ZyWALL IDP 10.

Why should I define Policy Check on WAN/LAN port?

Attacks could come from internal network (LAN) or from external network (Internet), therefore not only do you need to define policy check on WAN interface, but also on LAN interface.

What's Pre-defined signature?

Pre-defined signatures are signatures created by **ZyXEL Security Response Team (ZSRT)**. These signatures are attack patterns or misuse network behavior researched and studied by **ZSRT**, then compiled into a “pre-defined” policy set available for update.

Why should I need to update signature?

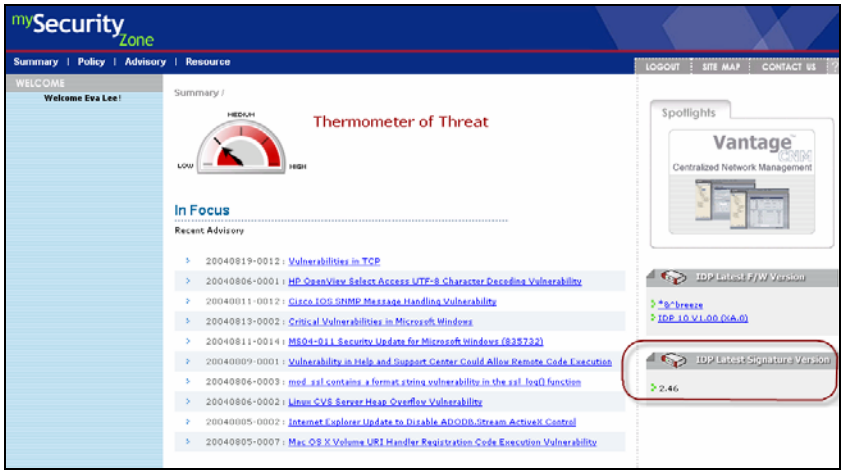
Intrusion detection is much like virus protection; an IDP system that hasn’t been updated for a year will miss common new attacks. **ZyXEL Security Respose Team (ZSRT)** will publish new “pre-defined” policy set on the policy update server (updateidp.zyxel.com). ZyWALL IDP10 is preset to download the latest policy every day automatically.

Where can I get the description of a policy or advisory?

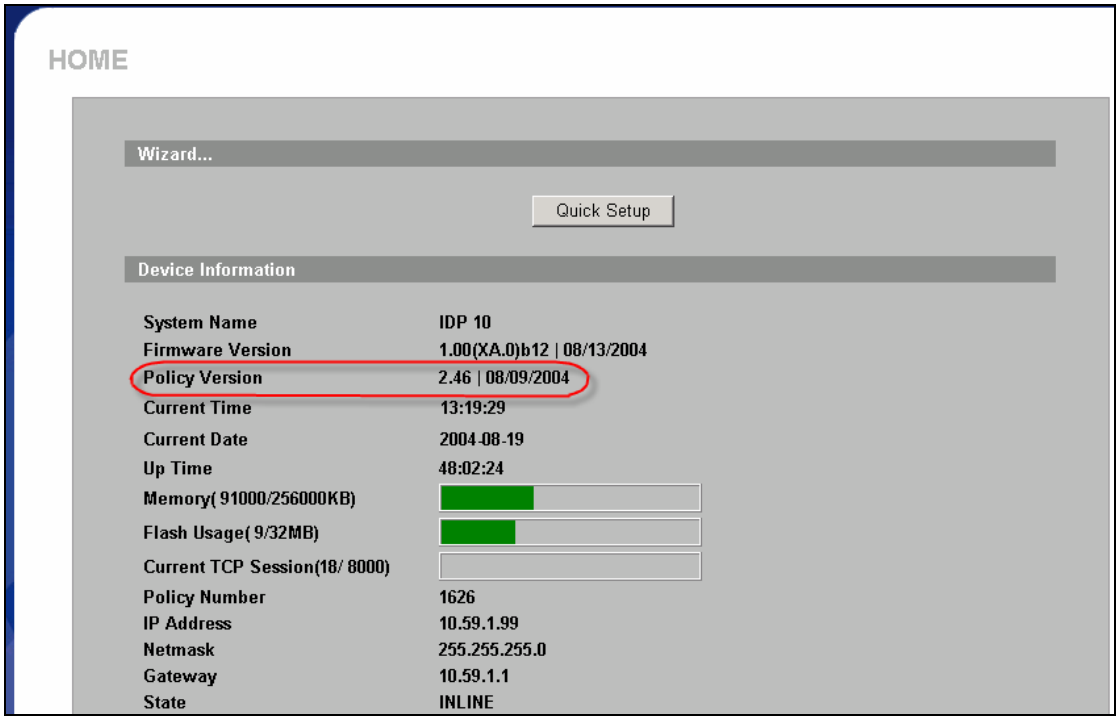
Whenever there are new advisories, policies published by ZyXEL, users can go to **mySecurityZone** (https://mysecurity.zyxel.com) to check the detailed description. The login user name/password is as login user name/password for http://www.myzyxel.com where users register ZyWALL IDP10.

How do I make sure my ZyWALL IDP10 already gets the latest policy?

You can check the latest policy version on **mySecurityZone (**https://mysecurity.zyxel.com)



And you should make sure your ZyWALL IDP 10 has updated policy to the latest version. Go to WEB Interface→Home.



I can't download the latest policy from update server. How can I fix the problem?

We recommend users to update policy, send E-mail reports or syslogs through ZyWALL IDP10's **MGMT** port (management port). Please make sure your ZyWALL IDP10 can go to Internet through **MGMT** port. If users insist to use **WAN** (or **LAN**) port to update policy, send E-mail reports or syslogs, then users need to turn off

stealth mode on WAN (or **LAN**) interface.

Additionally, since ZyWALL IDP10 downloads the latest policies periodically from the update server (updateidp.zyxel.com). DNS server should be configured correctly on ZyWALL IDP10 (**SYSTEM/GENEARL/Device/DNS Server**).

How many User-defined policies can I have on ZyWALL IDP 10?

You can create up to 128 User-defined policies on a ZyWALL IDP 10.

How many policies does ZyWALL IDP 10 support in total?

ZyWALL IDP 10 can contain up to 3000 policies, Pre-defined + User-defined.

Does configuration backup include Pre-defined/Updated signatures?

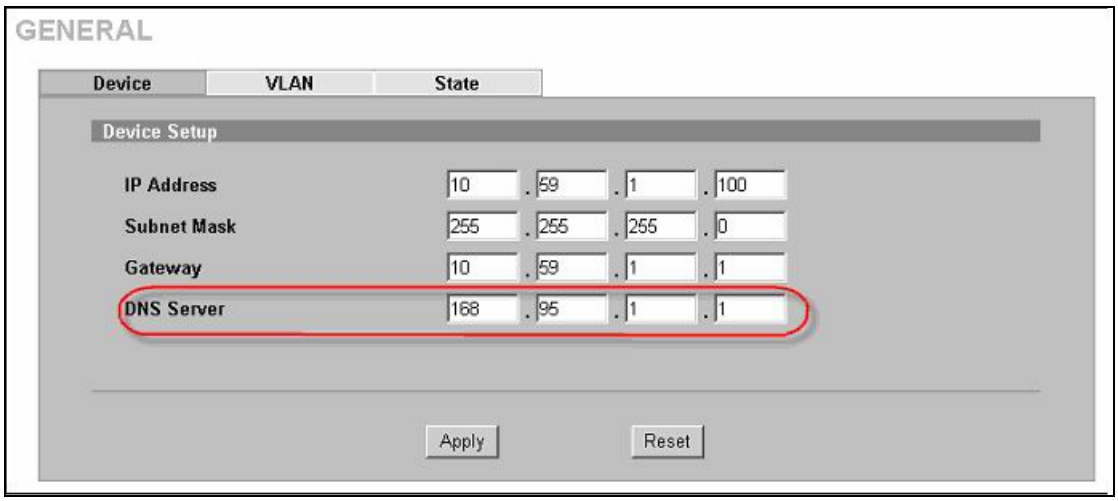
No, Pre-defined signatures will not backup when you perform a configuration backup. Only system parameters and User-defined signatures will be back up.

What's the default password of ZyWALL IDP10?

The default password to login ZyWALL IDP10 is "1234". For console login, the user name is "admin", password is also "1234".

Why can't I input mail server address by domain name?

You should configure DNS server's IP address first in
System>>General>>Device>>DNS Server



What's "Drop" and "Block Connection" for Action of User Defined Policy?

Action of "Drop", will drop the traffic that matches the defined policy silently. So the sender would not get any response or error/warning message about the action.

"Block Connection" is for TCP traffic, since UDP is a connectionless protocol. When users choose to Block the connection which matches the defined policy, then the device will send TCP Reset to the both ends of the TCP connection.

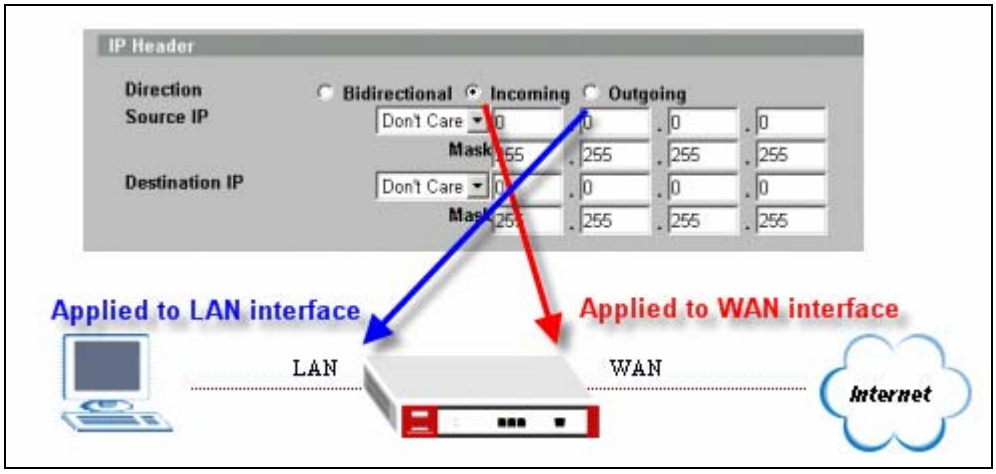
How to use URL String in Content setup of User-defined policy?

A **URL string** is a complete web site address. **Case sensitive** is any string where upper case and lower case letters are considered different.
The **URL string** is case insensitive, can include the character '?' and spaces and ignores character order. Therefore "/cgi-bin/foo.exe?p1=abc&p2=def" and "/cgi-bin/foo.exe?p2=def&p1=abc" are considered a match. Extra parameters in the payload don't matter either. For example, a pattern "/cgi-bin/foo.exe?p1=abc&p2=def" would match a packet with URL string "/cgi-bin/foo.exe?p0=xyz&p1=abc&p2=def".

What's the definition of "Incoming" and "Outgoing" direction in a policy setup?

A policy is bound to WAN or LAN interface when it's created. If the policy is created to check **Incoming** direction, then it's applied on **WAN** interface. If the policy is

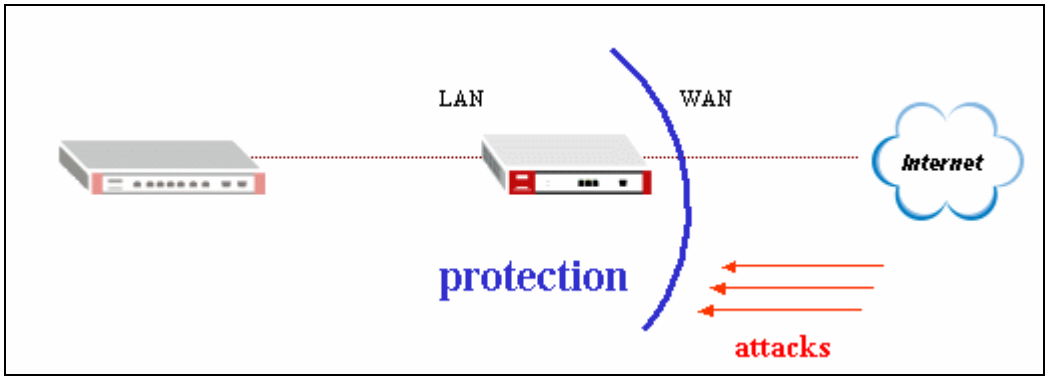
created to check **Outgoing** direction, it is applied on **LAN** interface. While a policy is set **Bi-directiona**l, it is applied on both **WAN** and **LAN** interfaces.



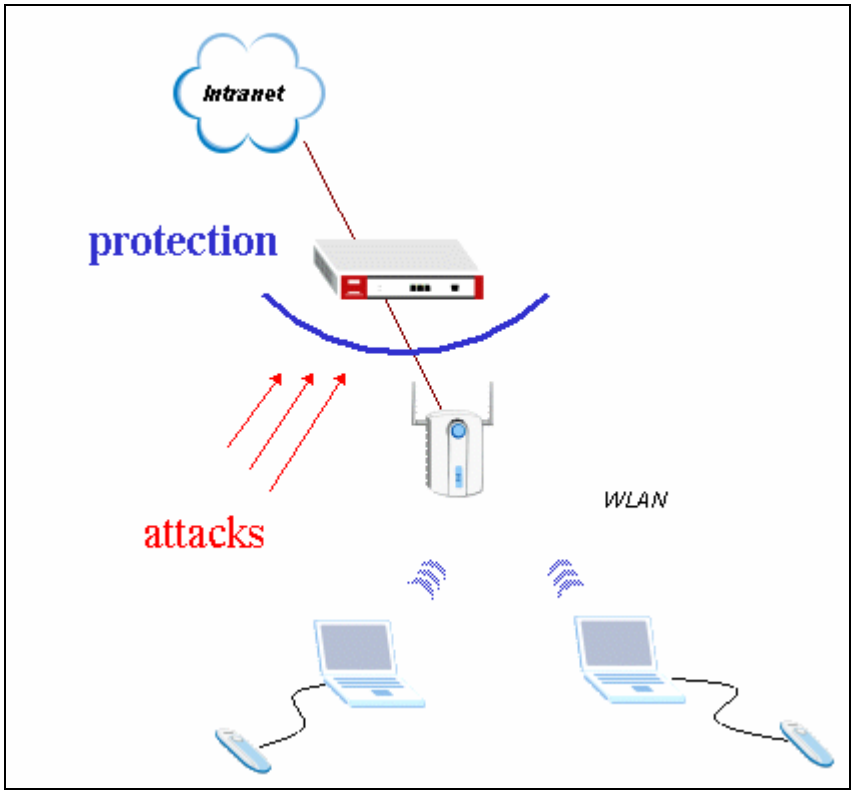
How to decide which Interface should be applied for policy check?

Users can setup policy check from **WEB GUI/SYSTEM/INTERFACE/Policy Check**. Policy check acts as a switch to enable or disable checking mechanism on WAN or LAN port. A policy is bound to either WAN or LAN interface based on the direction defined during setup. If you enable policy check on WAN interface, then the policies bound to WAN interface will be checked. However, if you disable policy check on LAN interface, then the policies bound to LAN interface won't be checked.

If your IDP is used to protect a trusted network from being attacked by Internet attackers, then you can disable policy check on LAN interface, and enable policy check on WAN interface. Thus Internet access traffic from trusted domain won't be checked.



If the IDP is placed on the entry point of a Wireless LAN network, we recommend you to apply policy check on the WAN interface, due to the lack of security protection of Wireless LAN.



In User-defined policy, what's the meaning of Matching Offset, Matching Depth?

Matching Offset defines the payload start point. If **Protocol** type is **IP**, then the matching starting point is at the end of the layer-3 header; otherwise, it would start matching from the end of the layer-4 header.
Matching Depth is the length of the payload to search for a match.
The Offset and Depth apply to all strings.

How does IDP check multiple contents?

For multiple contents, the order in which they're found doesn't matter (that is string 3 could be found before string 1 as long as it's within the depth defined) and string overlaps are also allowed. The multiple contents should be all found in one packet for a match.

What's the priority among Pre-defined policy and User-defined policy?

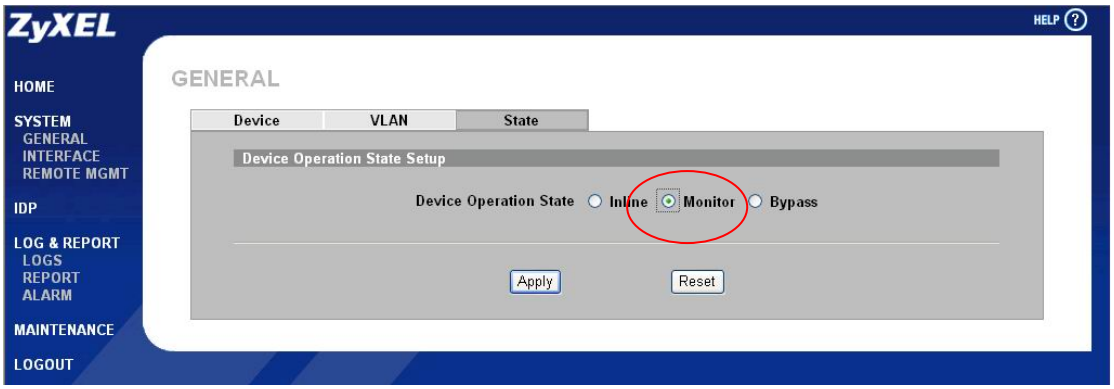
The User-defined policies are always checked before the Pre-defined policy.

Trouble Shooting

In this part we'll introduce the steps to trouble shoot when problems occur at customer side.

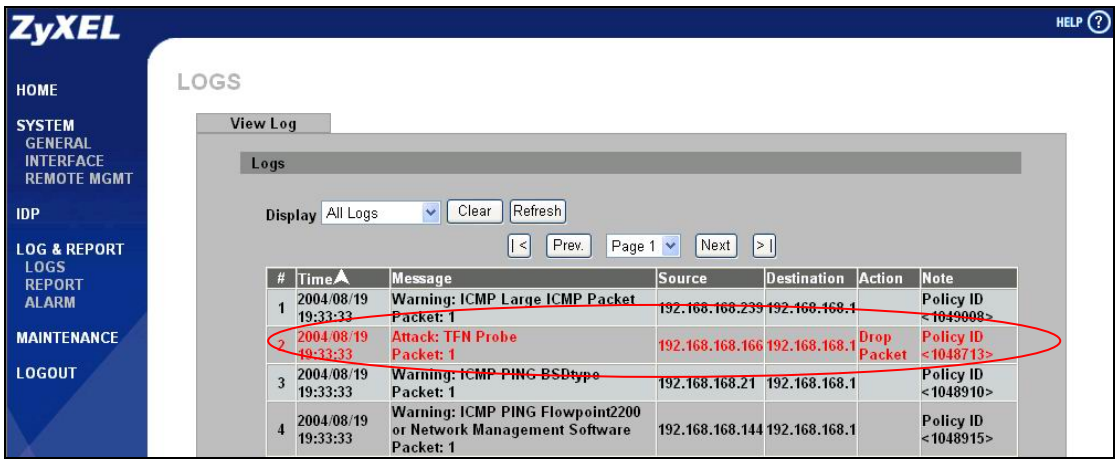
Unable to Run Applications

Step1. First of all, please switch your IDP to Monitor state and click Apply.

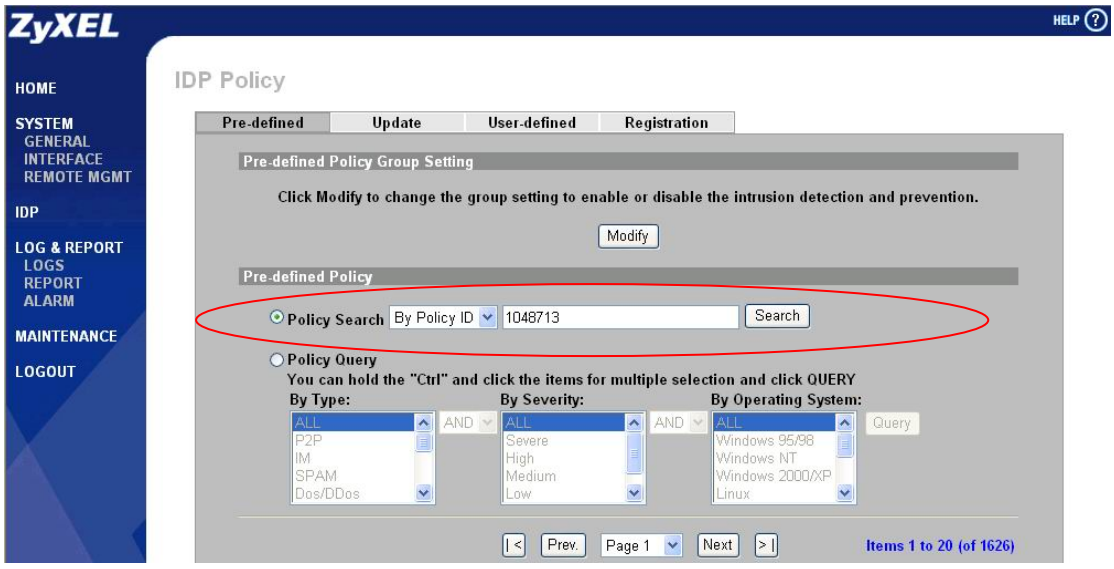


Step2. Try the application again. If it's still unable to run then it should be nothing to do with IDP 10. Please check settings of your application, PC, OS or other network devices. Otherwise, please go to the next step.

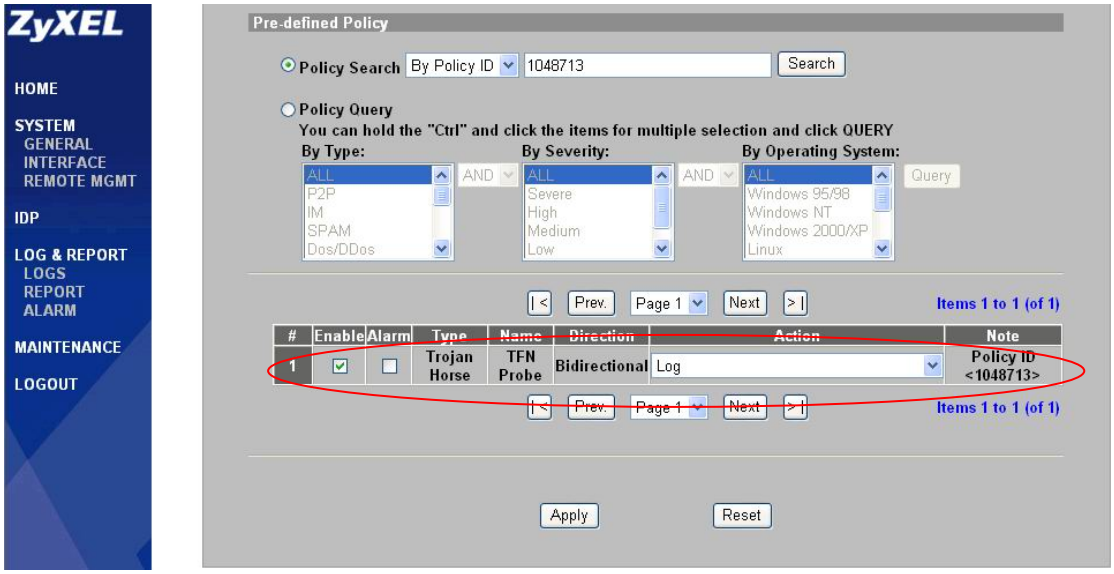
Step3. Go to WEB interface of ZyWALL IDP10, identify the False Positives policy in **Logs**. Then record down this Policy ID no.



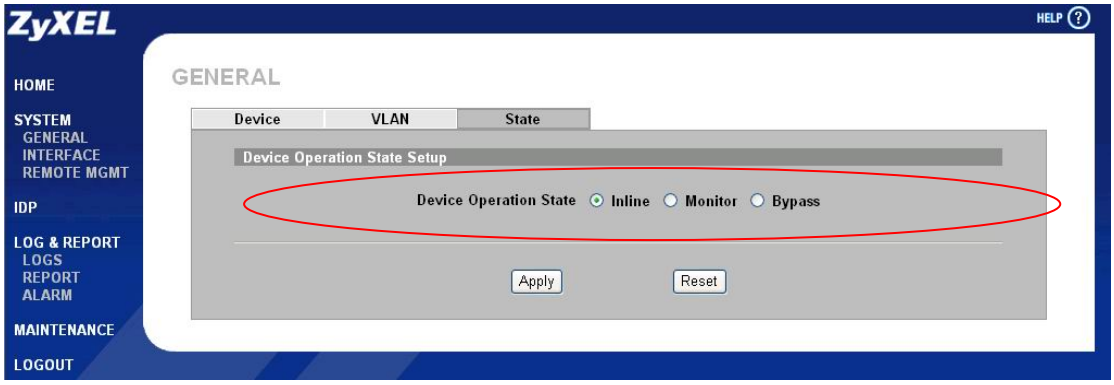
Step4. Search this policy by the Policy ID in **IDP>>Pre-defined>>Policy Search**.



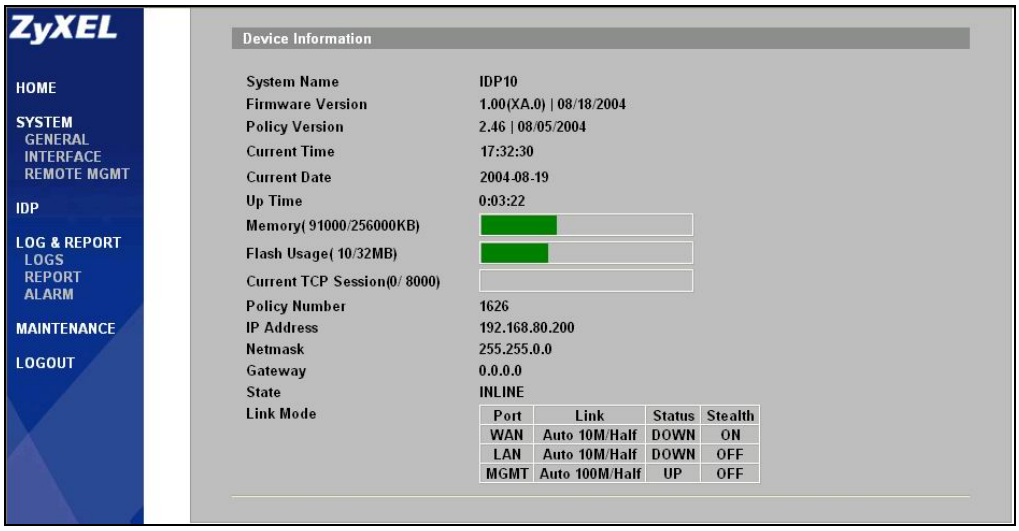
Step5. Under the search result, please change the Action taken to Log ONLY and click Apply.



Step6. Switch your IDP back to Inline state and activate them by clicking Apply. Then try to run the application again.



Step7. Finally, it should be able to run now. If possible, please provide us the application's name & version and the policy ID and system information including IDP 10's firmware version and policy version; it will be great help for us to trace the root cause.



Step8. If it was still unable to run then please repeat step 3, 4, 5 until identify and correct this False Positives policy.

CLI Command List

System related Command

Command					Description
set	log	logmax			Setup maximum log number the device generated every second
	system	passwd <value>			Setup login password
		system tomeout			Setup login idle timeout
		backup			Backup configuration
		restore			Restore configuration
		vlan	id		Setup vlan id
			link <UnTAg|Tag>		Enable/disable vlan tag
		ip <ip address>			Setup device ip address
		mask			Setup device subnet mask
		gateway			Setup device gateway ip address
		detect	vpnbypass <ON/OFF>		Enable/disable vpn packet bypass
			portscan <ON/OFF>		Enable/disable portscan function
			fragment <ON/OFF>		Enable/disable fragment function

			stateful <ON/OFF>		Enable/disable TCP state check
			integrity <ON/OFF>		Setup TCP idle timeout
			tcptimeout <value>		Setup maximum ping length
			pinglen <value>		Setup maximum ping packet number per second
			pingmax <value>	wan	Setup maximum ping packet accepted at wan port
				lan	Setup maximum ping packet accepted at lan port
			policy	wan <ON/OFF>	Setup policy check on/off wan port
				lan <ON/OFF>	Setup policy check on/off loan port
	interface	link	wan	10 <half/full>	Setup wan port speed 10/100; full/half duplex
				100 <half/full>	
				auto <half/full>	Enable auto negotiation
			lan	10 <half/full>	Setup lan port speed 10/100; full/half duplex
				100 <half/full>	
				auto <half/full>	Enable auto negotiation
		stealth	wan <ON/OFF>		Enable/disable stealth mode on wan port
			lan <ON/OFF>		Enable/disable stealth mode on lan port
	remote	snmp	on <LAN+MGMT/WAN+MGMT/MGMT/ALL>		Enable remote snmp access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port
			off		Disable remote snmp access
			acl <ip address>		Setup access control list ip address
			commnuity	ro <value>	Setup community read only string
				rw <value>	Setup community read/write string
				trap <value>	Setup snmp trap
			system name <value>		Setup remote snmp system name
			trap <ON/OFF>		Enable/disable remote snmp trap
			trap ip <value>		Setup remote snmp trap send to ip address
		ssh	on <CAN+MGMT/WAN+MGMT/MGMT/ALL>		Enable remote SSH access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port

			off		Disable remote SSH access
			acl <ip address>		Setup access control list ip address
		web	on <CAN+MGMT/WAN+MGMT/MGMT/ALL>		Enable remote web access from LAN+MGMT/WAN+MGMT/MGMT ONLY/ALL port
			off		Disable remote we access
			acl <ip address>		Setup access control list ip address
get	state				Get system state
	log				Get device log
	system				Get system information
	time				Get device time
	interface				Get interface information
	all				Get all information
	remote				Get remote access information
reboot					Reboot device
backup	tftp				Send file to TFTP server command
restore	tftp				Restore file from TFTP server
help					CLI help message
reset					Reset configuration to factory default
netstat					Display network state
ping					Ping
arp					Display arp information
exit					Logout system

Debug mode CLI Command

Command					Description
set	system	ip <ip>			Setup device temporary ip address in the debug mode
		mask <mask>			Setup device temporary ip mask in the debug mode
		gateway <gateway ip>			Setup device temporary ip gateway in the debug mode
		server <server ip >			Setup device temporary server ip address in the debug mode
upgrade	Tftp	<server ip>	<file name>		Using TFTP function to upgrade firmware
reboot					Reboot device
reset					Reset configuration to factory default
resetAll					Reset configuration to factory default, and delete all policies.
ping					Ping function
arp					Display arp information
netstat					Display network state